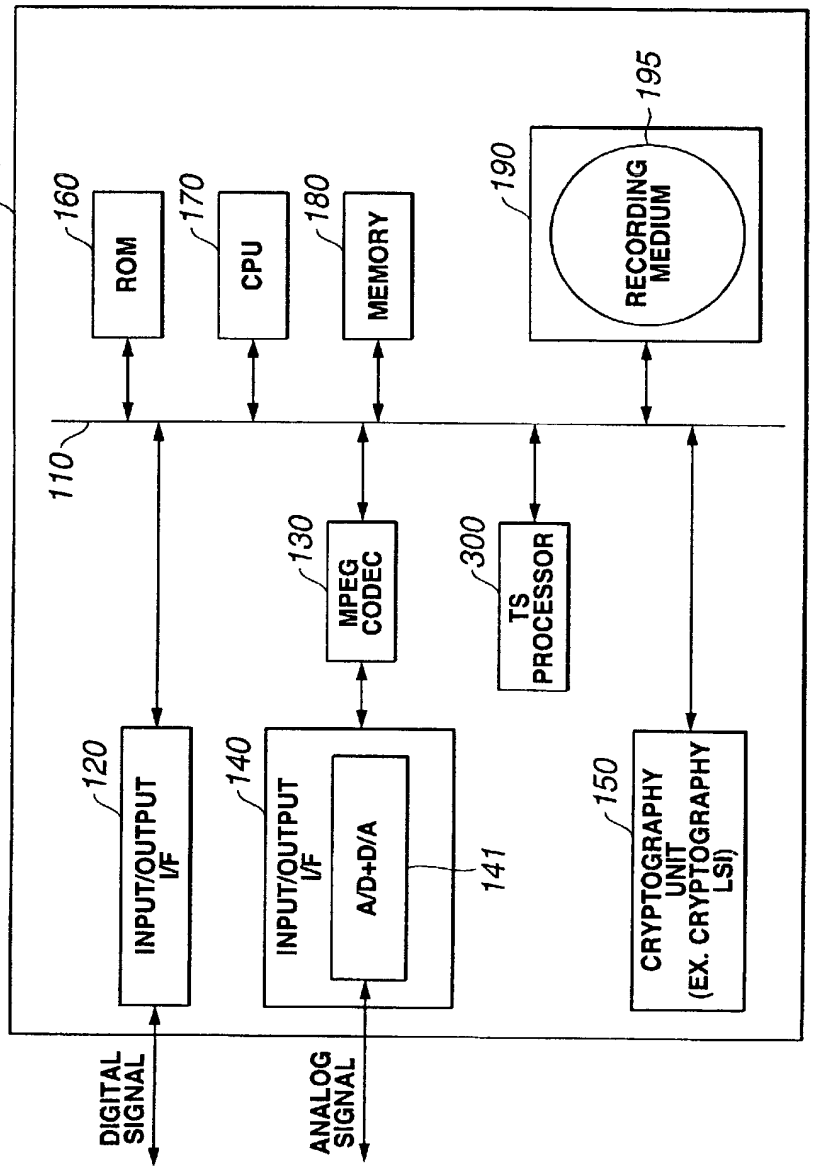

100
160
ROM
170
CPU
180
MEMORY
190
195
RECORDING MEDIUM
110
130
MPEG CODEC
300
TS PROCESSOR
120
INPUT/OUTPUT I/F
140
INPUT/OUTPUT I/F
A/D+D/A
141
150
CRYPTOGRAPHY UNIT (EX. CRYPTOGRAPHY LSI)
DIGITAL SIGNAL
ANALOG SIGNAL

FIG.1

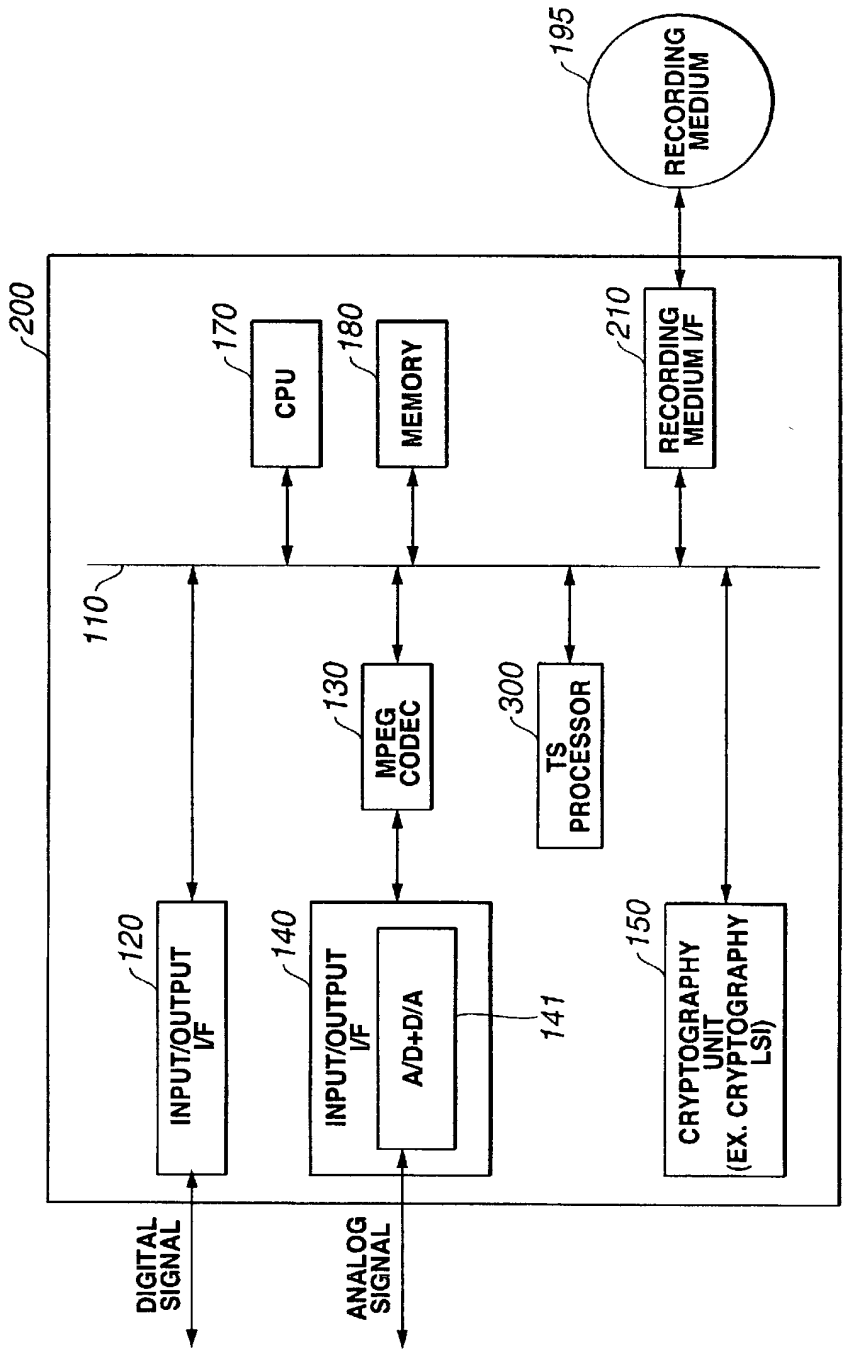

200
195
RECORDING MEDIUM
170
CPU
180
MEMORY
210
RECORDING MEDIUM I/F
110
130
MPEG CODEC
300
TS PROCESSOR
120
INPUT/OUTPUT I/F
140
INPUT/OUTPUT I/F
A/D+D/A
141
150
CRYPTOGRAPHY UNIT (EX. CRYPTOGRAPHY LSI)
DIGITAL SIGNAL
ANALOG SIGNAL

FIG.2

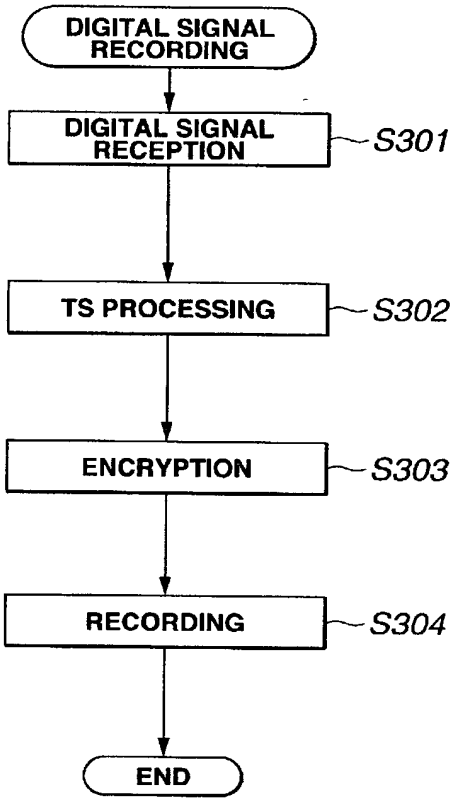

DIGITAL SIGNAL RECORDING
DIGITAL SIGNAL RECEPTION
S301
TS PROCESSING
S302
ENCRYPTION
S303
RECORDING
S304
END

FIG.3A

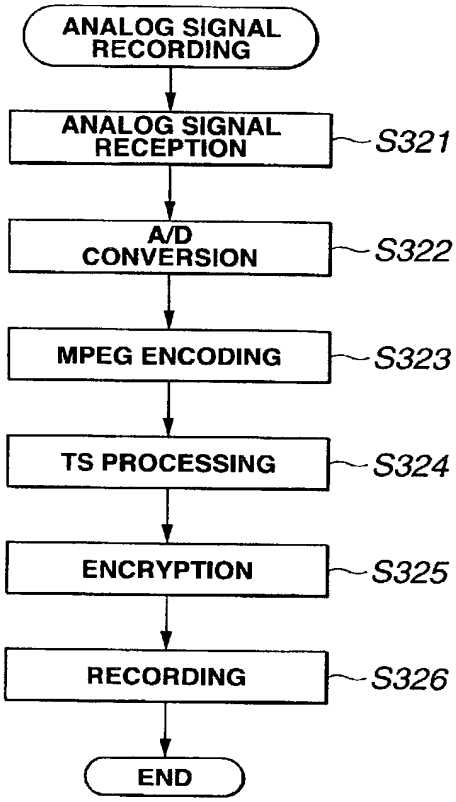

ANALOG SIGNAL RECORDING
ANALOG SIGNAL RECEPTION
S321
A/D CONVERSION
S322
MPEG ENCODING
S323
TS PROCESSING
S324
ENCRYPTION
S325
RECORDING
S326
END

FIG.3B

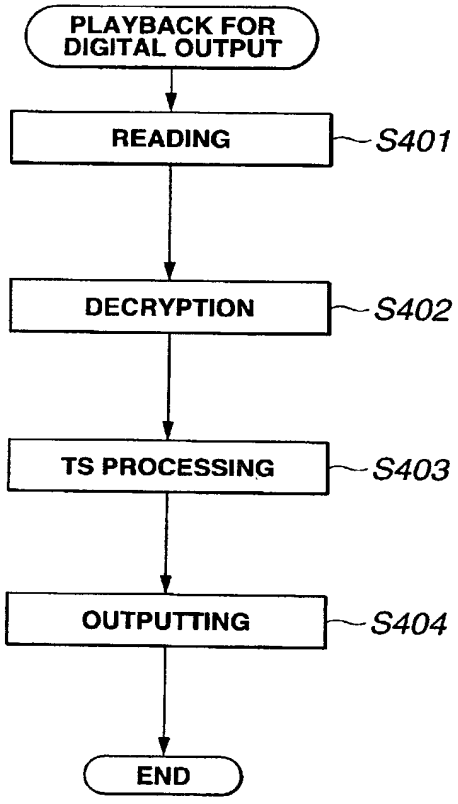

PLAYBACK FOR DIGITAL OUTPUT
READING
S401
DECRYPTION
S402
TS PROCESSING
S403
OUTPUTTING
S404
END

FIG.4A

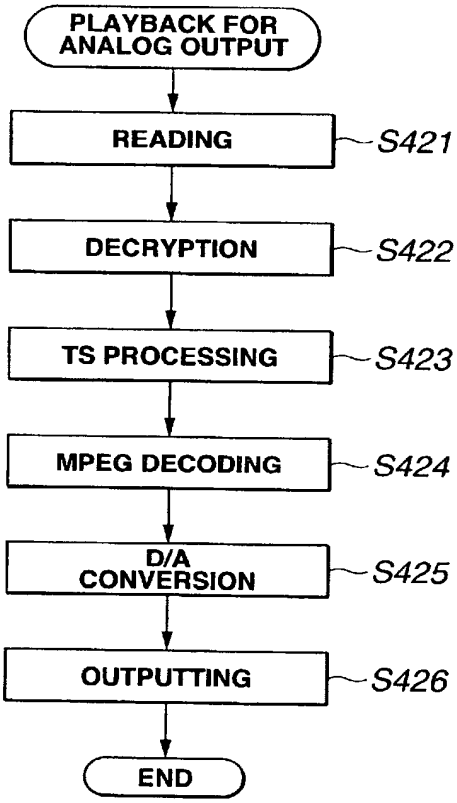

PLAYBACK FOR ANALOG OUTPUT
READING
S421
DECRYPTION
S422
TS PROCESSING
S423
MPEG DECODING
S424
D/A CONVERSION
S425
OUTPUTTING
S426
END

FIG.4B

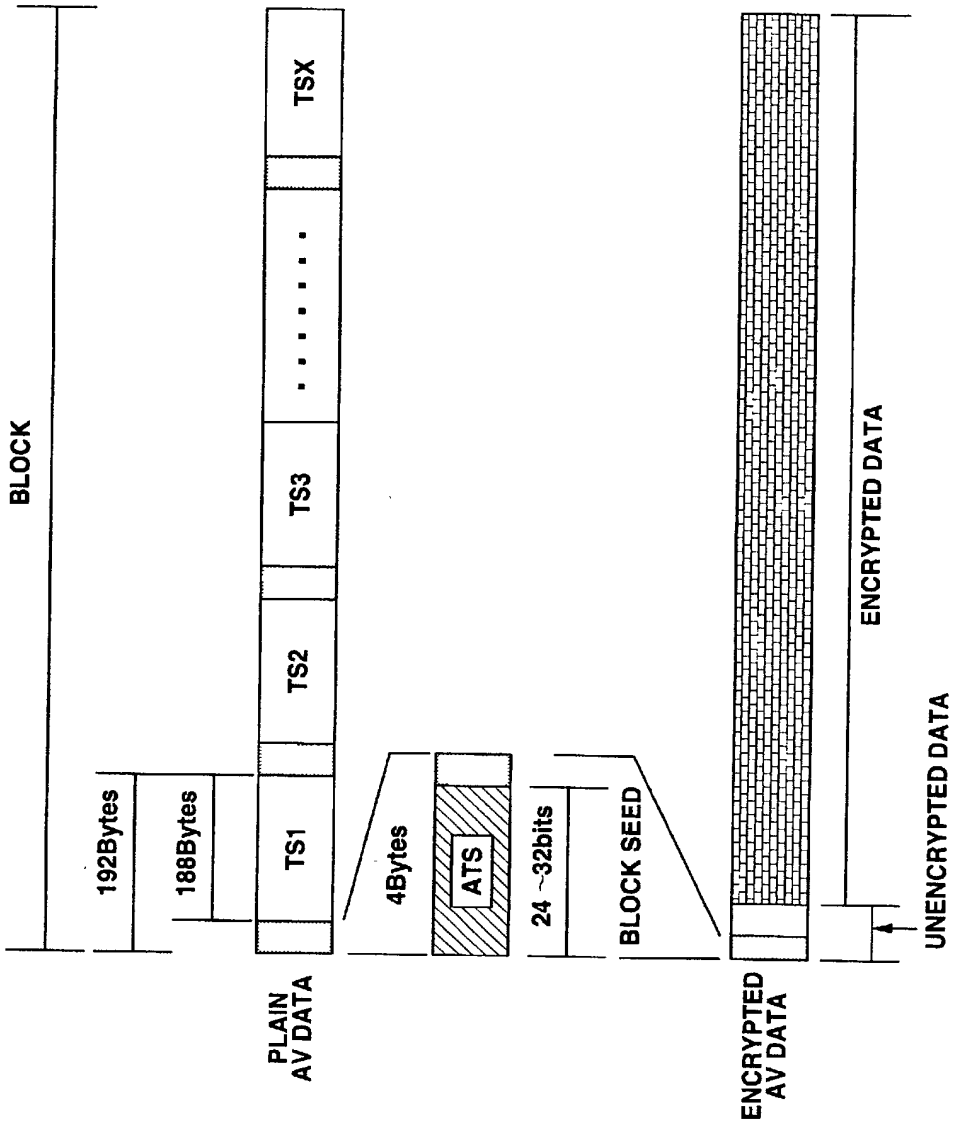

BLOCK
192Bytes
188Bytes
TS1
TS2
TS3
TSX
4Bytes
ATS
24 ~32bits
BLOCK SEED
PLAIN AV DATA
ENCRYPTED AV DATA
ENCRYPTED DATA
UNENCRYPTED DATA

FIG.5

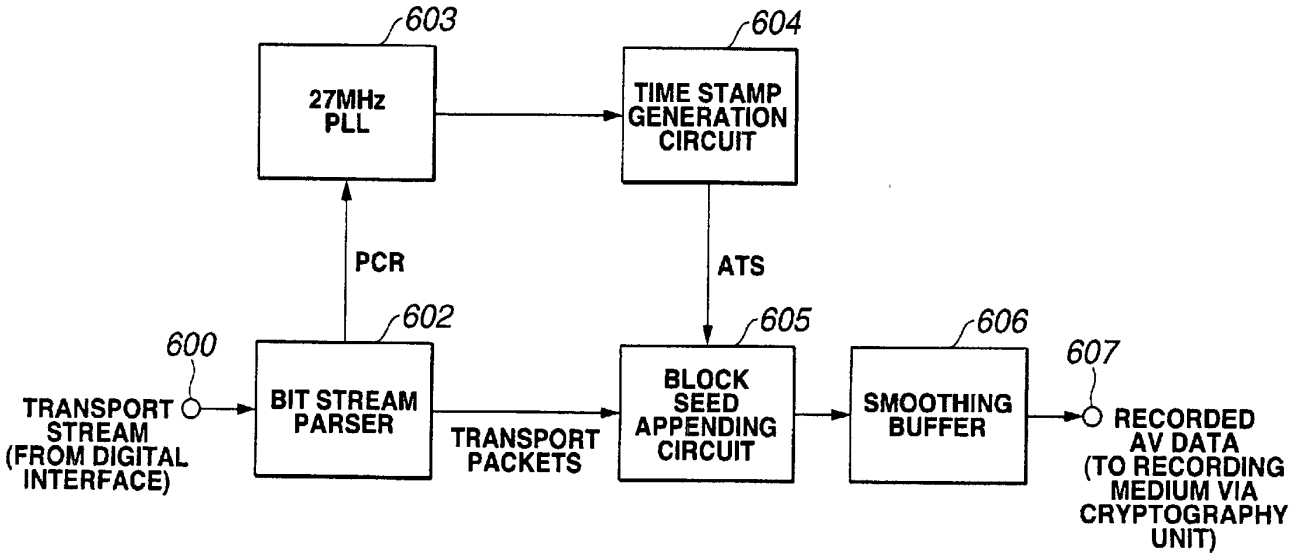

603
27MHz PLL
604
TIME STAMP GENERATION CIRCUIT
PCR
ATS
600
602
605
606
607
TRANSPORT STREAM (FROM DIGITAL INTERFACE)
BIT STREAM PARSER
TRANSPORT PACKETS
BLOCK SEED APPENDING CIRCUIT
SMOOTHING BUFFER
RECORDED AV DATA (TO RECORDING MEDIUM VIA CRYPTOGRAPHY UNIT)

FIG.6

FIG.7A
INPUT TRANSPORT STREAM

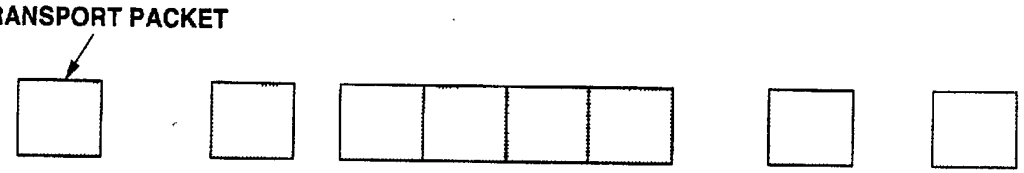


FIG.7B
OUTPUT OF BLOCK SEED APPENDING CIRCUIT

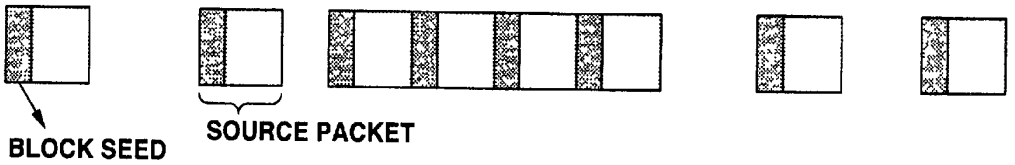
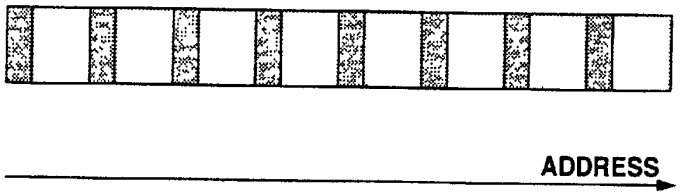


FIG.7C
AV DATA ON RECORDING MEDIUM



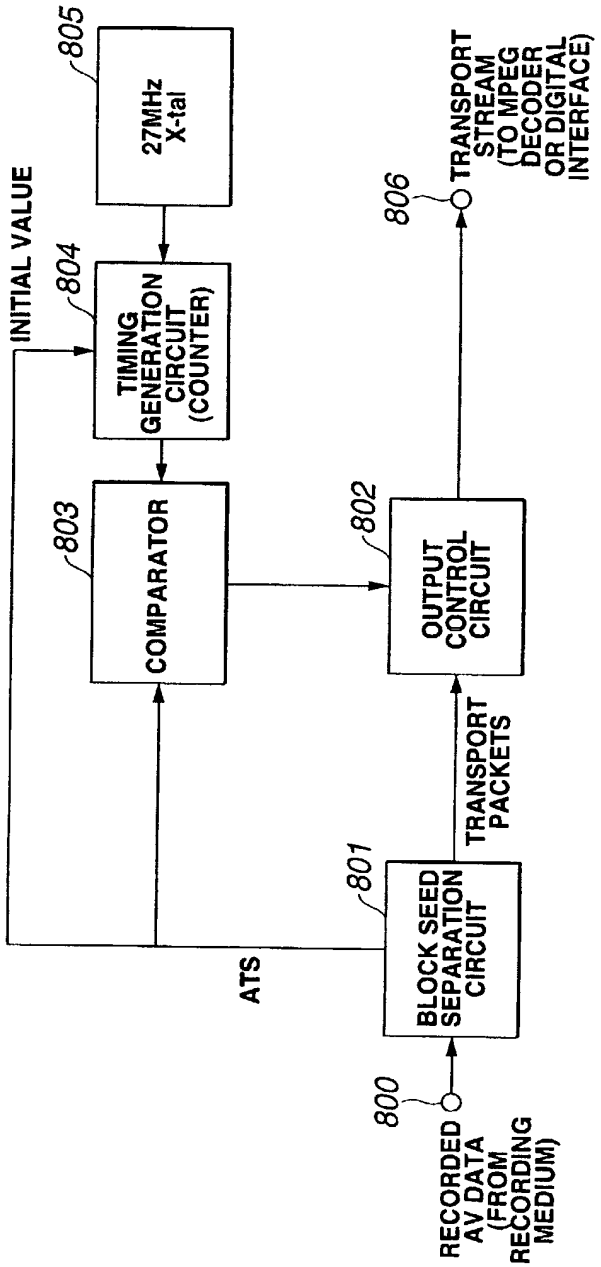

800
RECORDED AV DATA (FROM RECORDING MEDIUM)
801
BLOCK SEED SEPARATION CIRCUIT
TRANSPORT PACKETS
802
OUTPUT CONTROL CIRCUIT
803
COMPARATOR
804
TIMING GENERATION CIRCUIT (COUNTER)
805
27MHz X-tal
806
TRANSPORT STREAM (TO MPEG DECODER OR DIGITAL INTERFACE)
INITIAL VALUE
ATS

FIG.8

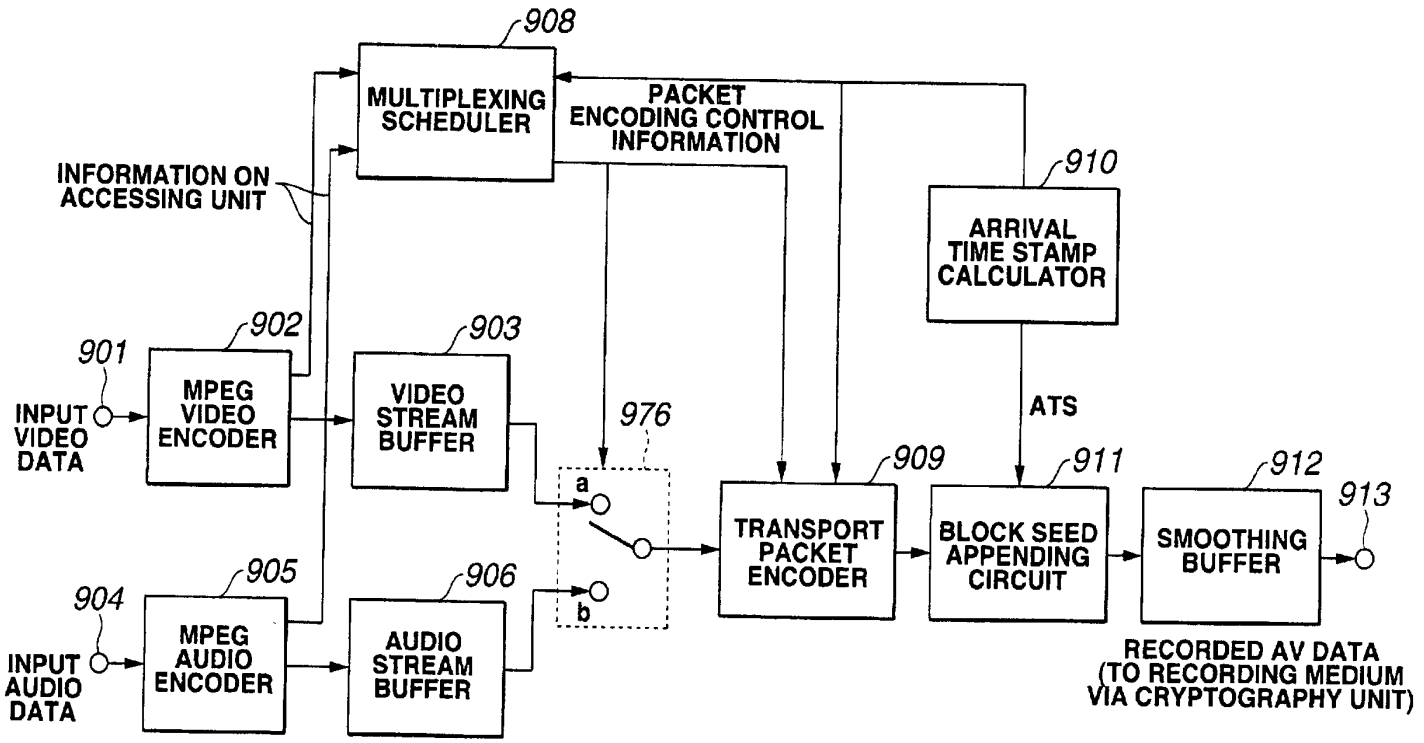

908
MULTIPLEXING SCHEDULER
PACKET ENCODING CONTROL INFORMATION
INFORMATION ON ACCESSING UNIT
910
ARRIVAL TIME STAMP CALCULATOR
901
902
903
INPUT VIDEO DATA
MPEG VIDEO ENCODER
VIDEO STREAM BUFFER
976
ATS
909
911
912
913
a
b
TRANSPORT PACKET ENCODER
BLOCK SEED APPENDING CIRCUIT
SMOOTHING BUFFER
904
905
906
INPUT AUDIO DATA
MPEG AUDIO ENCODER
AUDIO STREAM BUFFER
RECORDED AV DATA
(TO RECORDING MEDIUM
VIA CRYPTOGRAPHY UNIT)

FIG.9

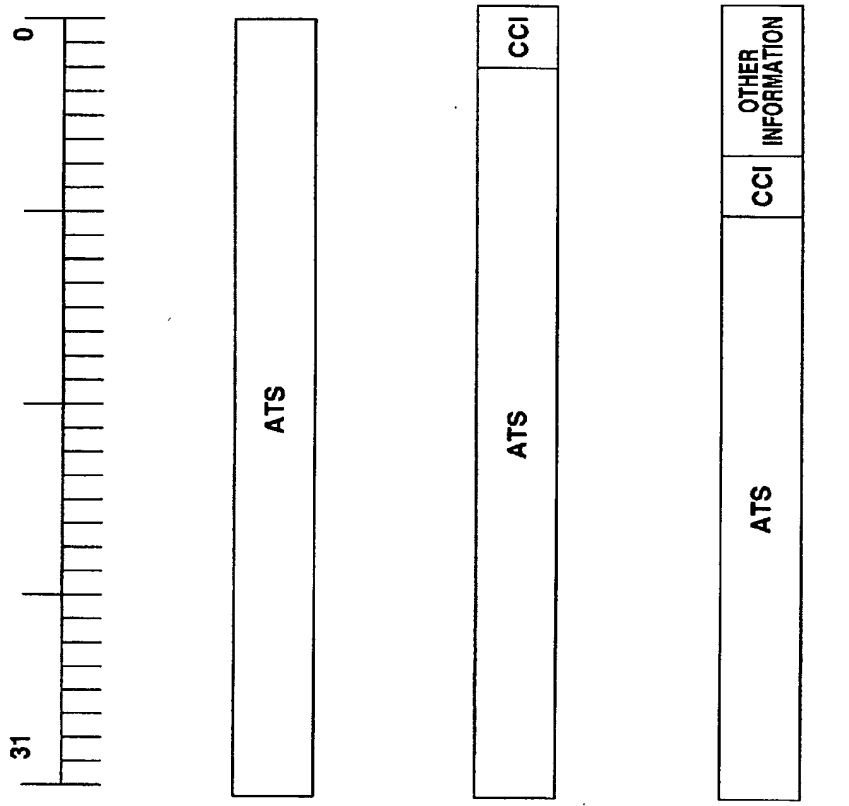

31
0
BLOCK SEED
ATS
EXAMPLE 1:
ATS OF 32BITS
ATS
CCI
EXAMPLE 2:
ATS OF 30 BITS
AND CCI OF 2BITS
ATS
CCI
OTHER INFORMATION
EXAMPLE 3:
ATS OF 24BITS,
CCI OF 2 BITS
AND OTHER
INFORMATION
OF 6 BITS

FIG.10

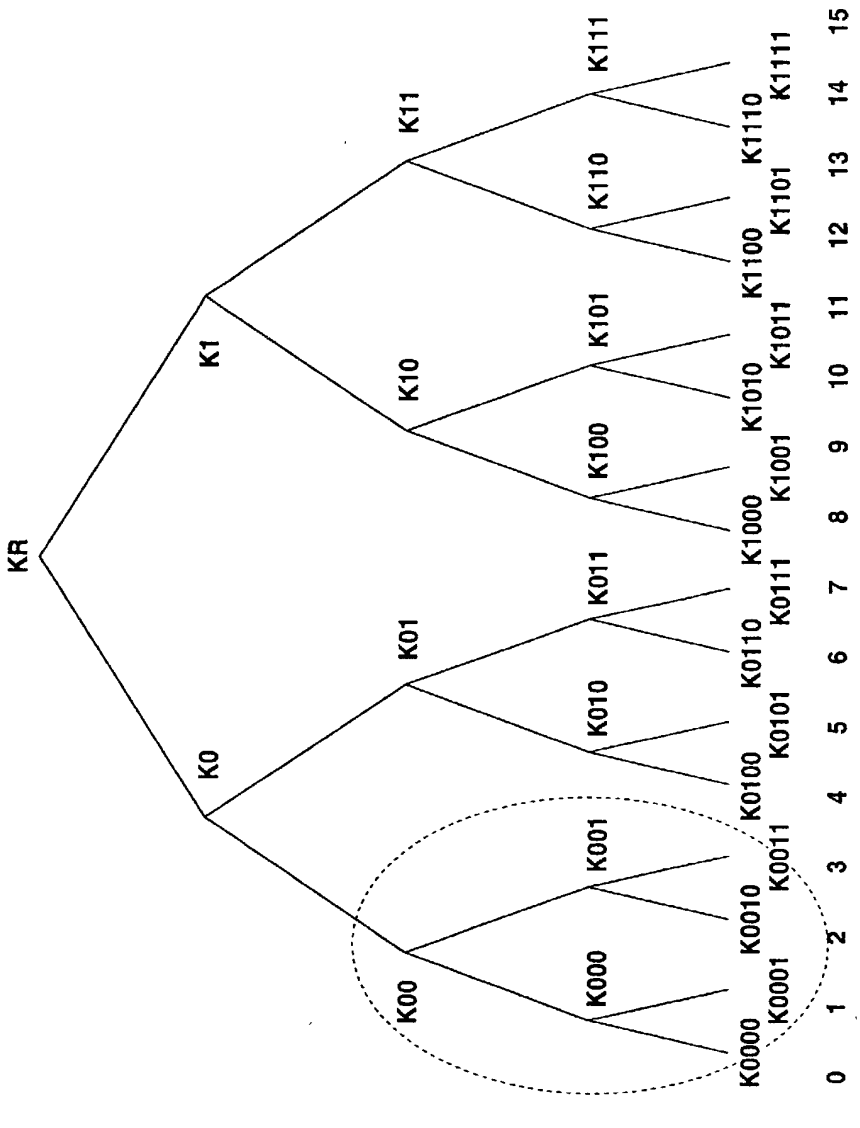

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
DEVICE

FIG.11

GENERATION : t	
INDEX	ENCRYPTION KEY
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG.12A

GENERATION : t	
INDEX	ENCRYPTION KEY
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG.12B

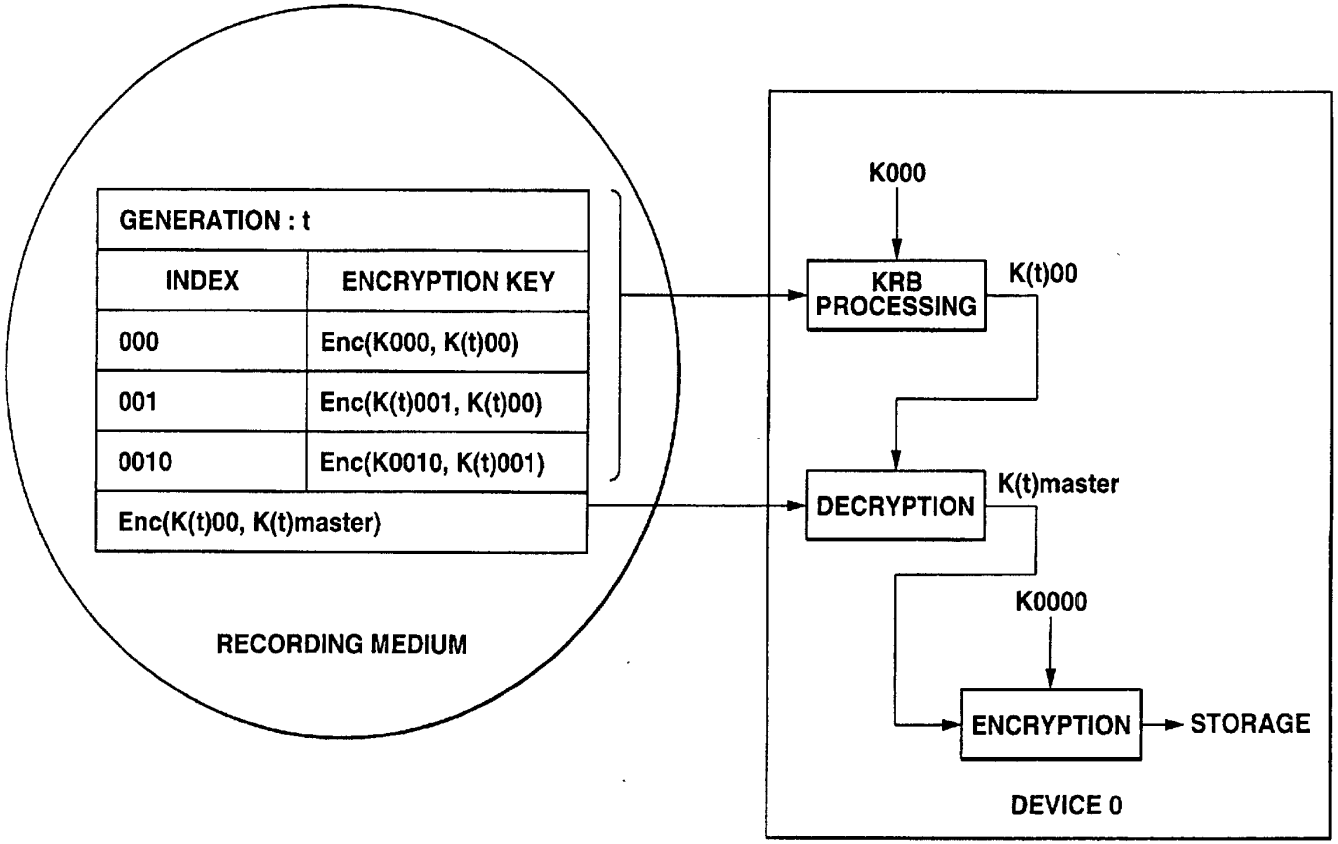

GENERATION : t
INDEX
ENCRYPTION KEY
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)master)
RECORDING MEDIUM
K000
KRB PROCESSING
K(t)00
DECRYPTION
K(t)master
K0000
ENCRYPTION
STORAGE
DEVICE 0

FIG.13

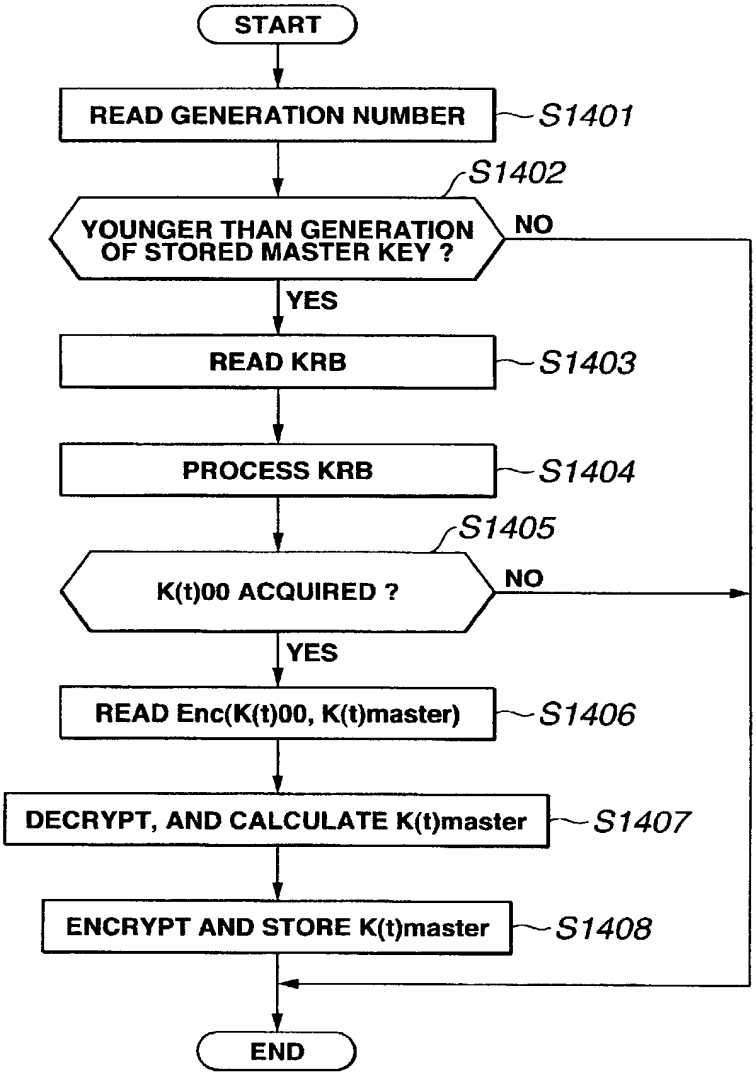

START
READ GENERATION NUMBER
S1401
S1402
YOUNGER THAN GENERATION OF STORED MASTER KEY ?
NO
YES
READ KRB
S1403
PROCESS KRB
S1404
S1405
K(t)00 ACQUIRED ?
NO
YES
READ Enc(K(t)00, K(t)master)
S1406
DECRYPT, AND CALCULATE K(t)master
S1407
ENCRYPT AND STORE K(t)master
S1408
END

FIG.14

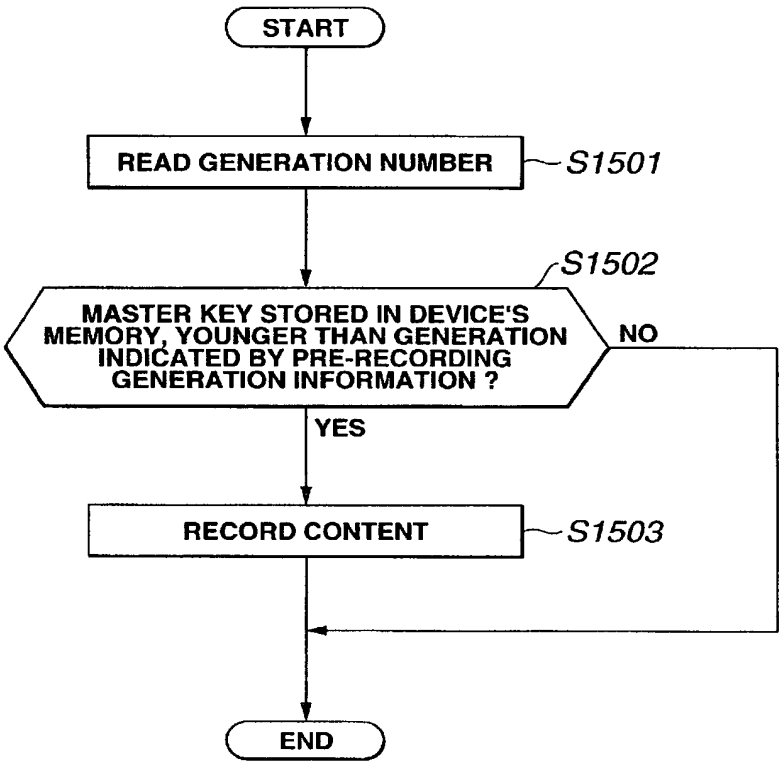

START
READ GENERATION NUMBER
S1501
S1502
MASTER KEY STORED IN DEVICE'S MEMORY, YOUNGER THAN GENERATION INDICATED BY PRE-RECORDING GENERATION INFORMATION ?
NO
YES
RECORD CONTENT
S1503
END

FIG.15

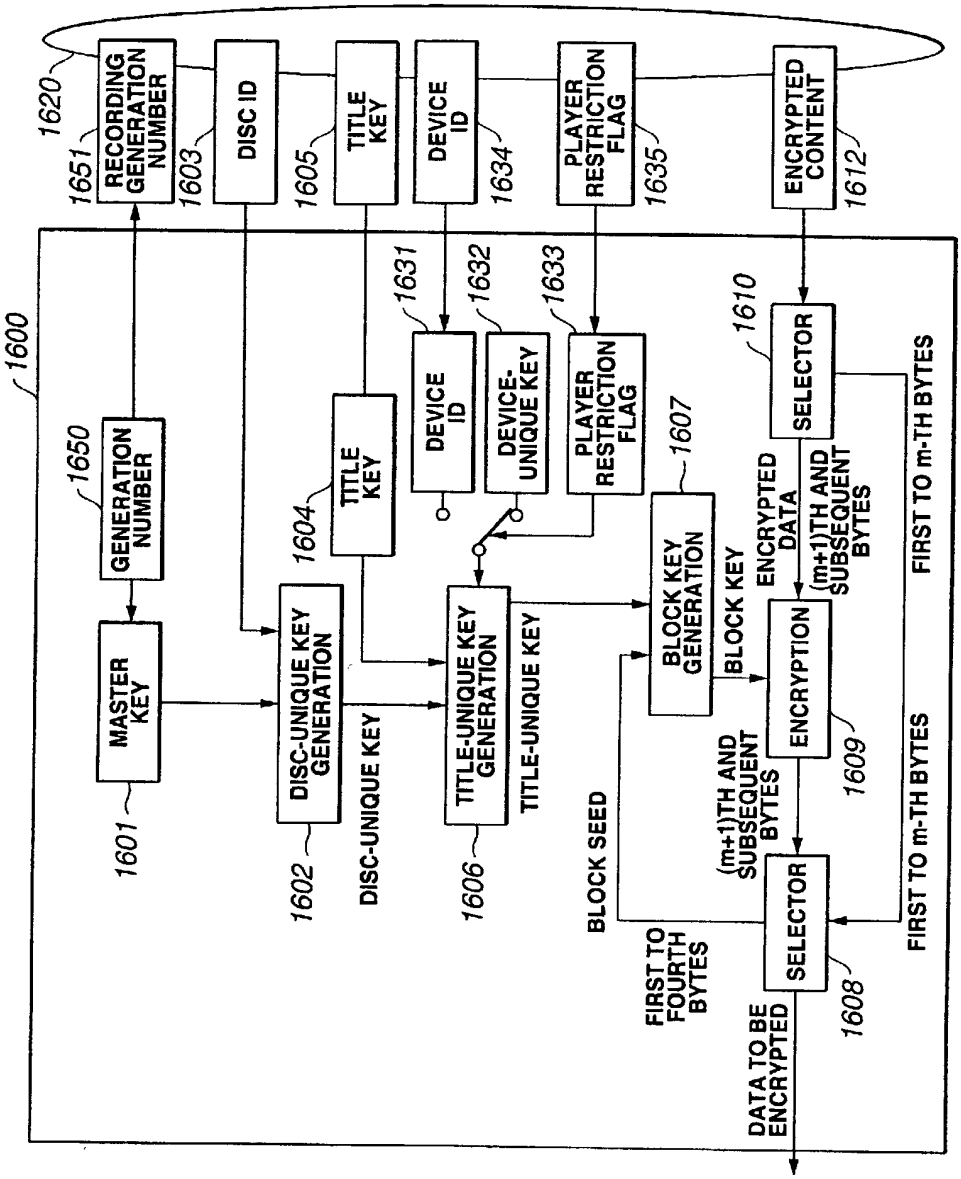

1600
1620
RECORDING GENERATION NUMBER
1651
DISC ID
1603
TITLE KEY
1605
DEVICE ID
1634
PLAYER RESTRICTION FLAG
1635
ENCRYPTED CONTENT
1612
GENERATION NUMBER
1650
MASTER KEY
1601
DISC-UNIQUE KEY GENERATION
1602
DISC-UNIQUE KEY
TITLE KEY
1604
TITLE-UNIQUE KEY GENERATION
1606
TITLE-UNIQUE KEY
DEVICE ID
1631
DEVICE-UNIQUE KEY
1632
PLAYER RESTRICTION FLAG
1633
BLOCK KEY GENERATION
1607
BLOCK KEY
SELECTOR
1610
ENCRYPTED DATA
(m+1)TH AND SUBSEQUENT BYTES
ENCRYPTION
1609
(m+1)TH AND SUBSEQUENT BYTES
BLOCK SEED
FIRST TO FOURTH BYTES
SELECTOR
1608
DATA TO BE ENCRYPTED
FIRST TO m-TH BYTES
FIRST TO m-TH BYTES

FIG.16

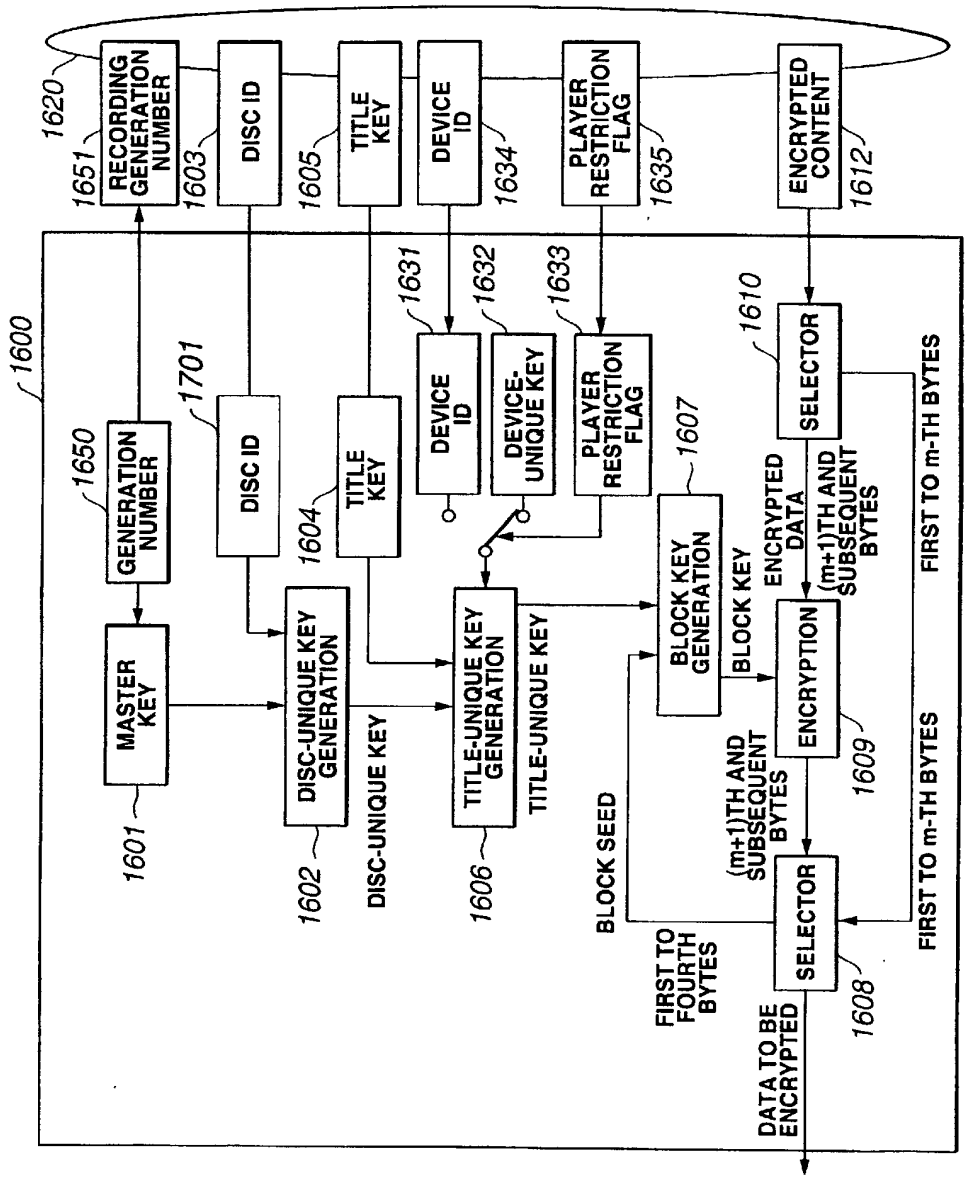

1600
1620
1651
RECORDING GENERATION NUMBER
1603
DISC ID
1605
TITLE KEY
1634
DEVICE ID
1635
PLAYER RESTRICTION FLAG
1612
ENCRYPTED CONTENT
1650
GENERATION NUMBER
1701
DISC ID
1604
TITLE KEY
1631
DEVICE ID
1632
DEVICE-UNIQUE KEY
1633
PLAYER RESTRICTION FLAG
1607
1610
SELECTOR
MASTER KEY
1601
DISC-UNIQUE KEY GENERATION
1602
DISC-UNIQUE KEY
TITLE-UNIQUE KEY GENERATION
1606
TITLE-UNIQUE KEY
BLOCK KEY GENERATION
BLOCK KEY
ENCRYPTED DATA
(m+1)TH AND SUBSEQUENT BYTES
ENCRYPTION
1609
BLOCK SEED
(m+1)TH AND SUBSEQUENT BYTES
FIRST TO FOURTH BYTES
SELECTOR
1608
DATA TO BE ENCRYPTED
FIRST TO m-TH BYTES
FIRST TO m-TH BYTES

FIG.17

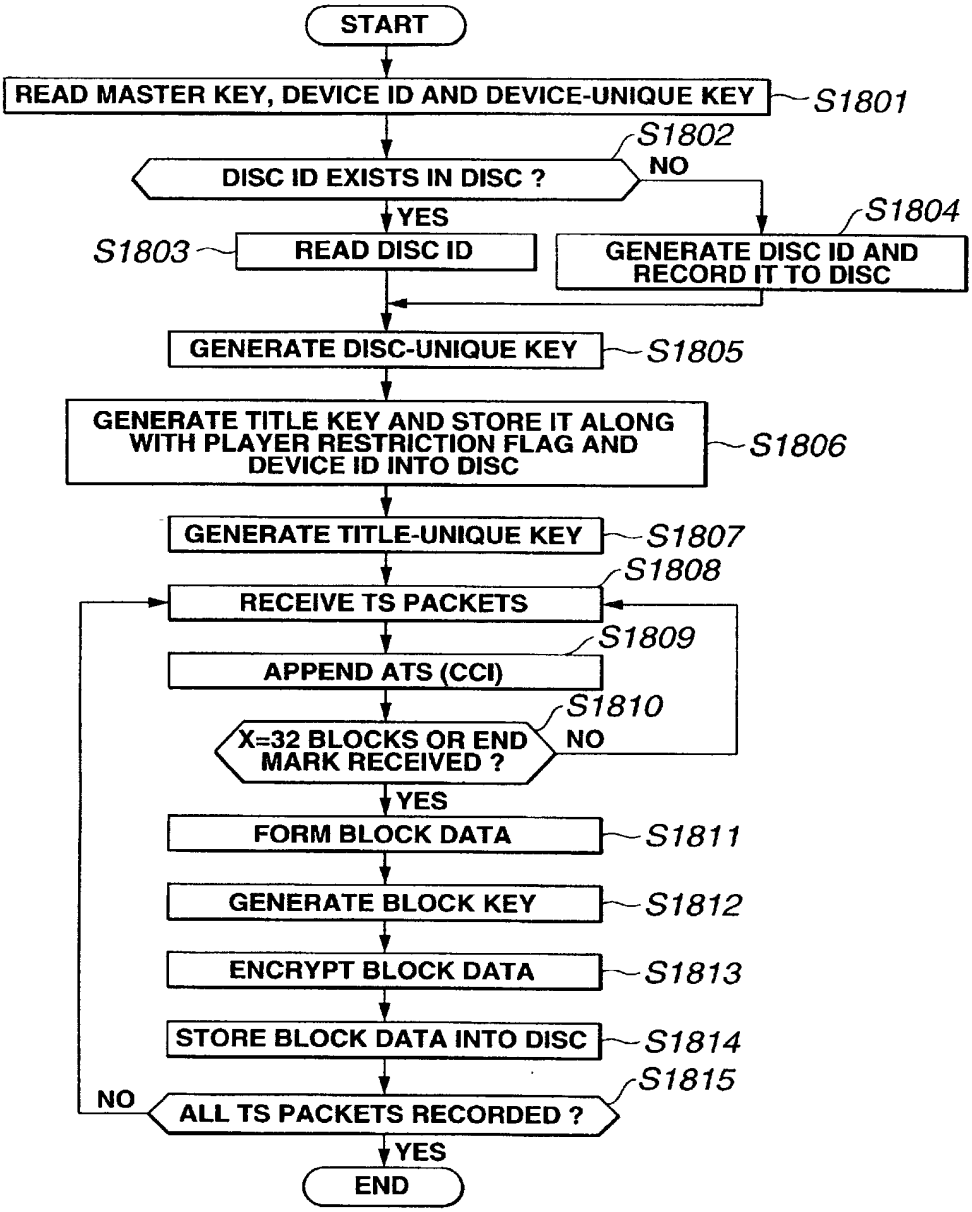
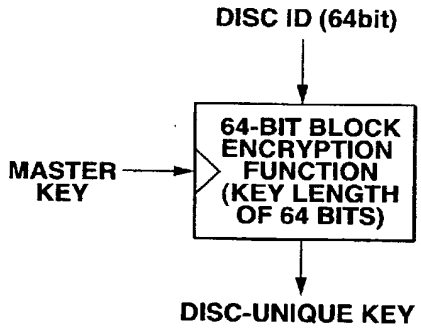

START
READ MASTER KEY, DEVICE ID AND DEVICE-UNIQUE KEY
S1801
S1802
DISC ID EXISTS IN DISC ?
NO
YES
S1803
READ DISC ID
S1804
GENERATE DISC ID AND RECORD IT TO DISC
GENERATE DISC-UNIQUE KEY
S1805
GENERATE TITLE KEY AND STORE IT ALONG WITH PLAYER RESTRICTION FLAG AND DEVICE ID INTO DISC
S1806
GENERATE TITLE-UNIQUE KEY
S1807
S1808
RECEIVE TS PACKETS
S1809
APPEND ATS (CCI)
S1810
X=32 BLOCKS OR END MARK RECEIVED ?
NO
YES
FORM BLOCK DATA
S1811
GENERATE BLOCK KEY
S1812
ENCRYPT BLOCK DATA
S1813
STORE BLOCK DATA INTO DISC
S1814
S1815
NO
ALL TS PACKETS RECORDED ?
YES
END

FIG.18

EXAMPLE 1

EXAMPLE OF DEVICE-UNIQUE KEY GENERATION

INPUTS:
MASTER KEY (64BITS)
DISC ID (64BITS)



EXAMPLE 2

OUTPUTS:
DISC-UNIQUE KEY (64BITS)

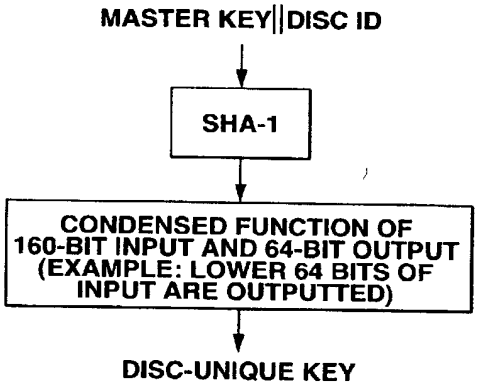


FIG.19

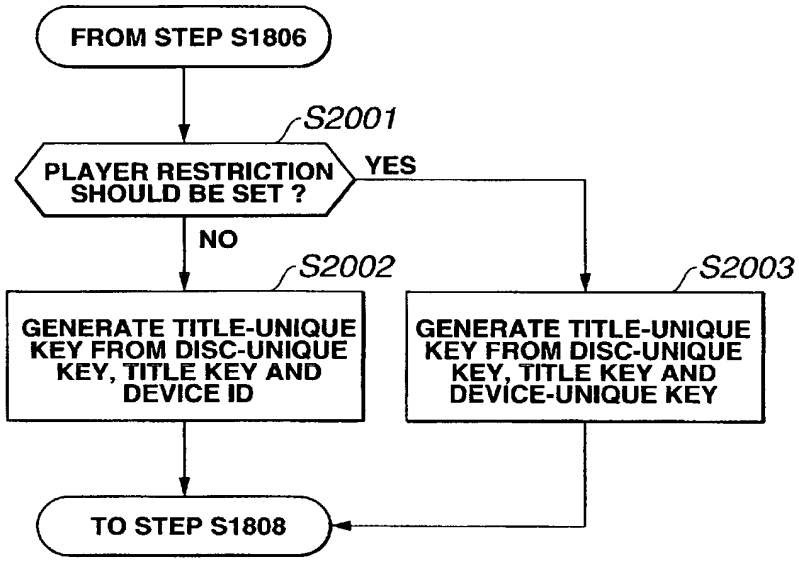

FROM STEP S1806
S2001
PLAYER RESTRICTION SHOULD BE SET ?
YES
NO
S2002
GENERATE TITLE-UNIQUE KEY FROM DISC-UNIQUE KEY, TITLE KEY AND DEVICE ID
S2003
GENERATE TITLE-UNIQUE KEY FROM DISC-UNIQUE KEY, TITLE KEY AND DEVICE-UNIQUE KEY
TO STEP S1808

FIG.20

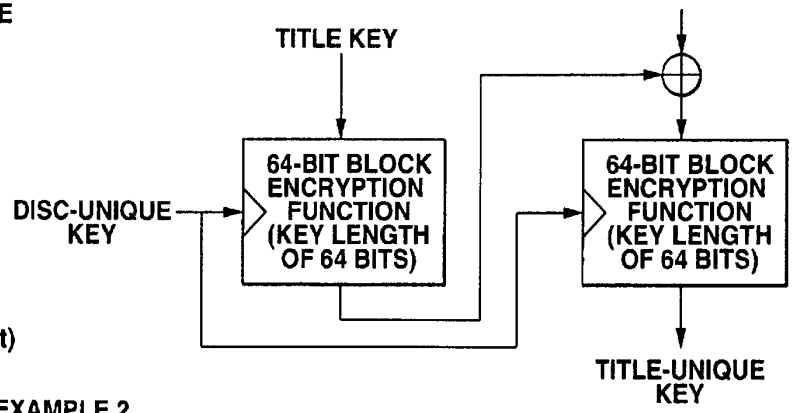
EXAMPLE 1

EXAMPLE OF TITLE-UNIQUE KEY GENERATION

INPUTS:

DISC-UNIQUE KEY (64bit)
TITLE KEY (64bit)

DISC ID (64bit) OR
DEVICE-UNIQUE KEY (64bit)



EXAMPLE 2

OUTPUTS:
TITLE-UNIQUE KEY (64BITS)

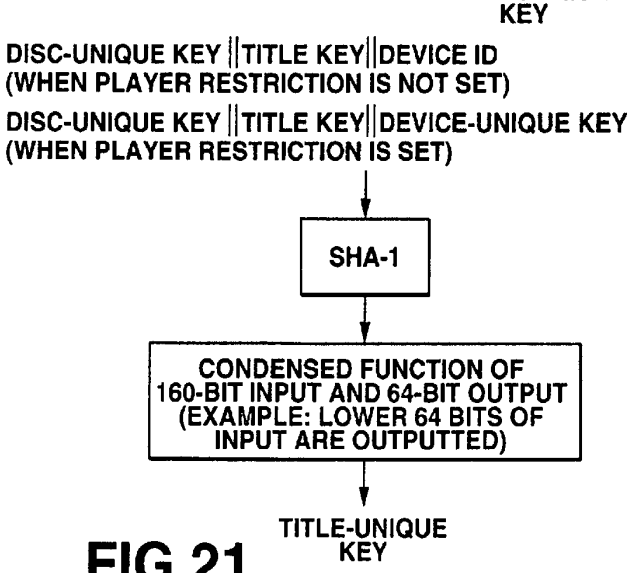
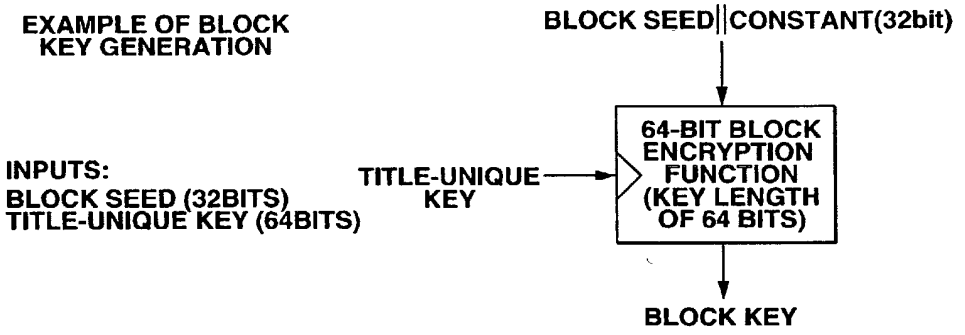


FIG.21

EXAMPLE 1

EXAMPLE OF BLOCK KEY GENERATION

INPUTS:
BLOCK SEED (32BITS)
TITLE-UNIQUE KEY (64BITS)



EXAMPLE 2

OUTPUTS:
BLOCK KEY (64BITS)

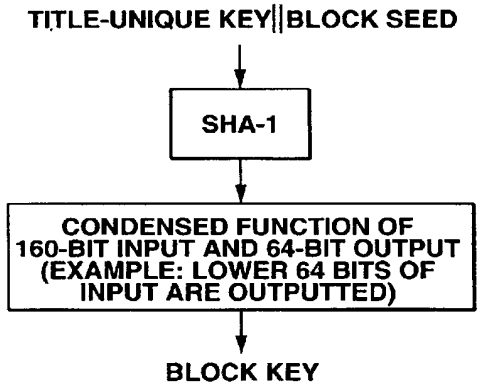


FIG.22

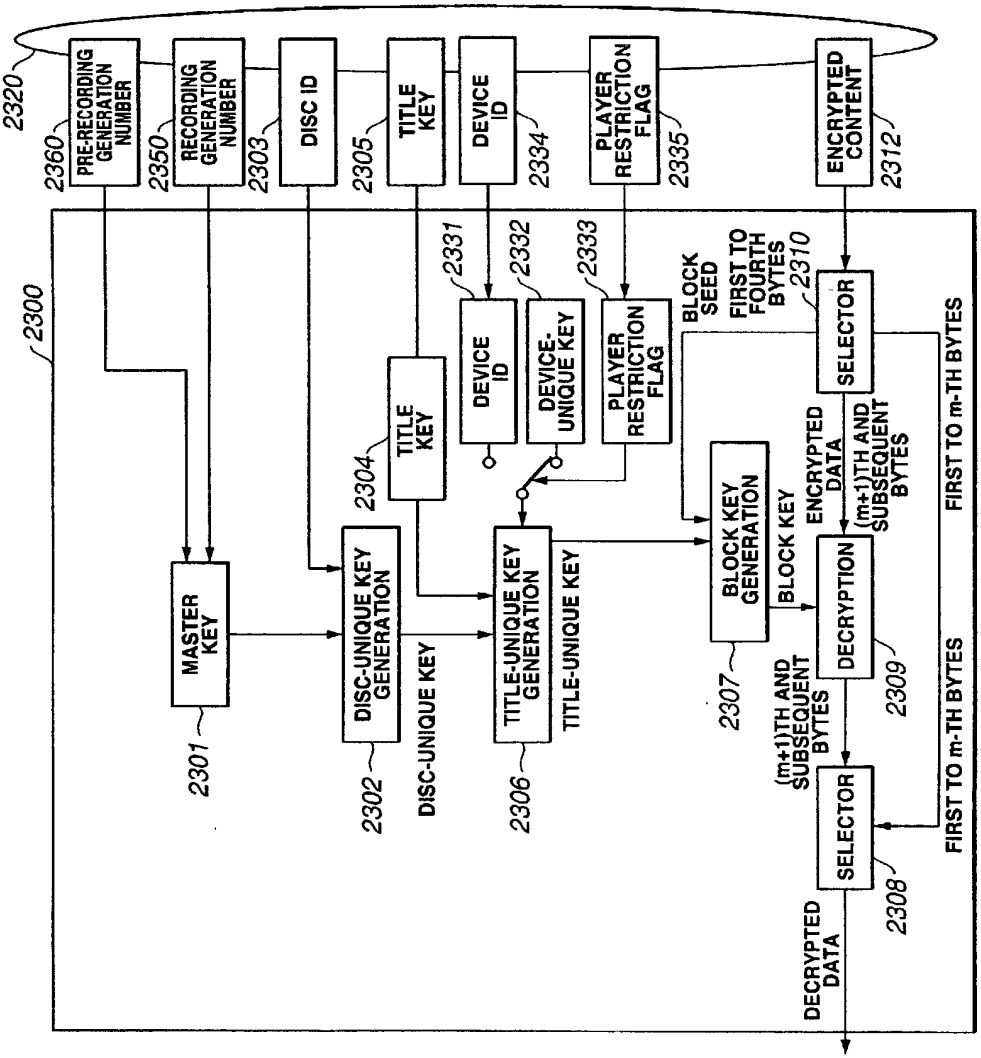

2320
PRE-RECORDING GENERATION NUMBER
2360
RECORDING GENERATION NUMBER
2350
DISC ID
2303
TITLE KEY
2305
DEVICE ID
2334
PLAYER RESTRICTION FLAG
2335
ENCRYPTED CONTENT
2312
2300
2331
2332
2333
BLOCK SEED
FIRST TO FOURTH BYTES
2310
SELECTOR
TITLE KEY
2304
DEVICE ID
DEVICE-UNIQUE KEY
PLAYER RESTRICTION FLAG
BLOCK KEY GENERATION
2307
BLOCK KEY
ENCRYPTED DATA
(m+1)TH AND SUBSEQUENT BYTES
MASTER KEY
2301
DISC-UNIQUE KEY GENERATION
2302
DISC-UNIQUE KEY
TITLE-UNIQUE KEY GENERATION
2306
TITLE-UNIQUE KEY
DECRYPTION
2309
(m+1)TH AND SUBSEQUENT BYTES
FIRST TO m-TH BYTES
FIRST TO m-TH BYTES
SELECTOR
2308
DECRYPTED DATA

FIG.23

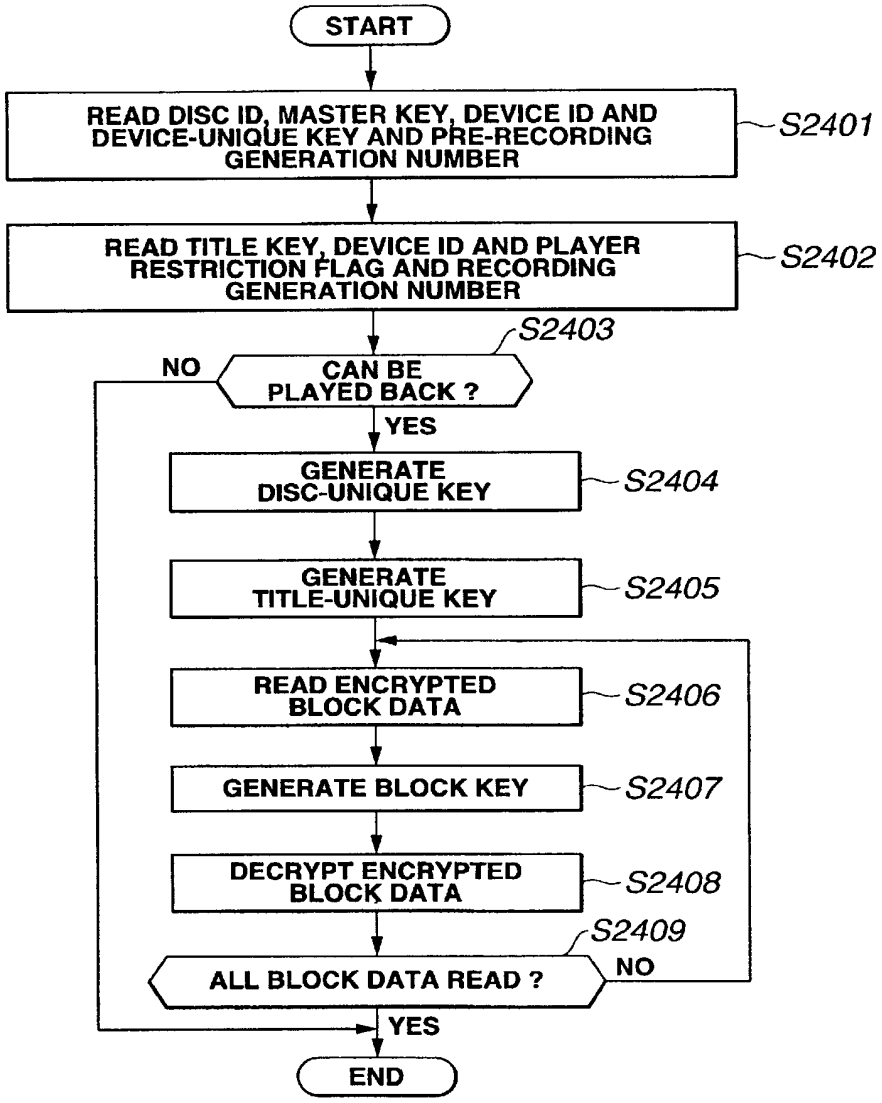

START
READ DISC ID, MASTER KEY, DEVICE ID AND DEVICE-UNIQUE KEY AND PRE-RECORDING GENERATION NUMBER
S2401
READ TITLE KEY, DEVICE ID AND PLAYER RESTRICTION FLAG AND RECORDING GENERATION NUMBER
S2402
S2403
CAN BE PLAYED BACK ?
NO
YES
GENERATE DISC-UNIQUE KEY
S2404
GENERATE TITLE-UNIQUE KEY
S2405
READ ENCRYPTED BLOCK DATA
S2406
GENERATE BLOCK KEY
S2407
DECRYPT ENCRYPTED BLOCK DATA
S2408
S2409
ALL BLOCK DATA READ ?
NO
YES
END

FIG.24

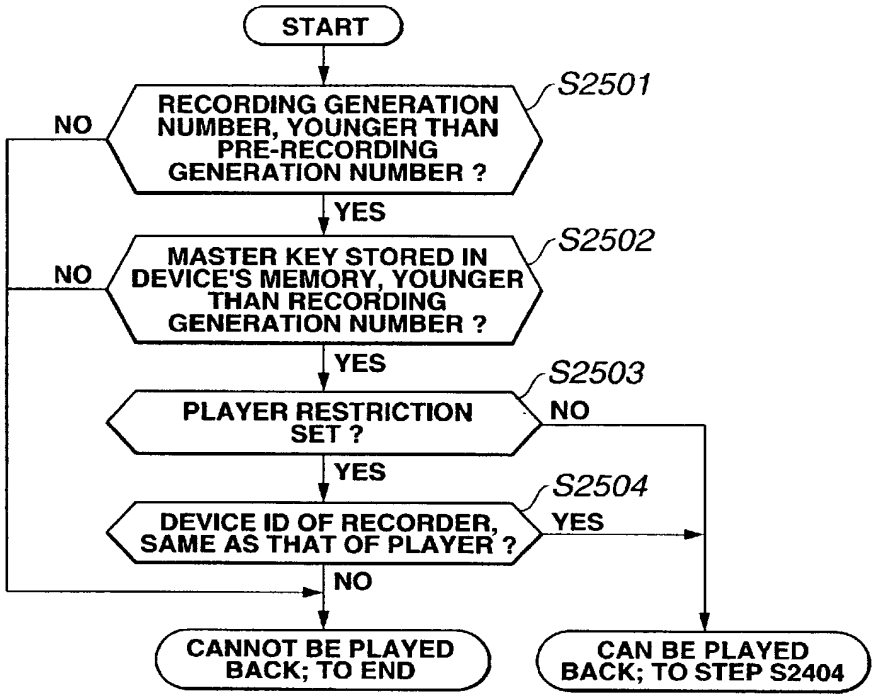

START
S2501
RECORDING GENERATION NUMBER, YOUNGER THAN PRE-RECORDING GENERATION NUMBER ?
NO
YES
S2502
MASTER KEY STORED IN DEVICE'S MEMORY, YOUNGER THAN RECORDING GENERATION NUMBER ?
NO
YES
S2503
PLAYER RESTRICTION SET ?
NO
YES
S2504
DEVICE ID OF RECORDER, SAME AS THAT OF PLAYER ?
YES
NO
CANNOT BE PLAYED BACK; TO END
CAN BE PLAYED BACK; TO STEP S2404

FIG.25

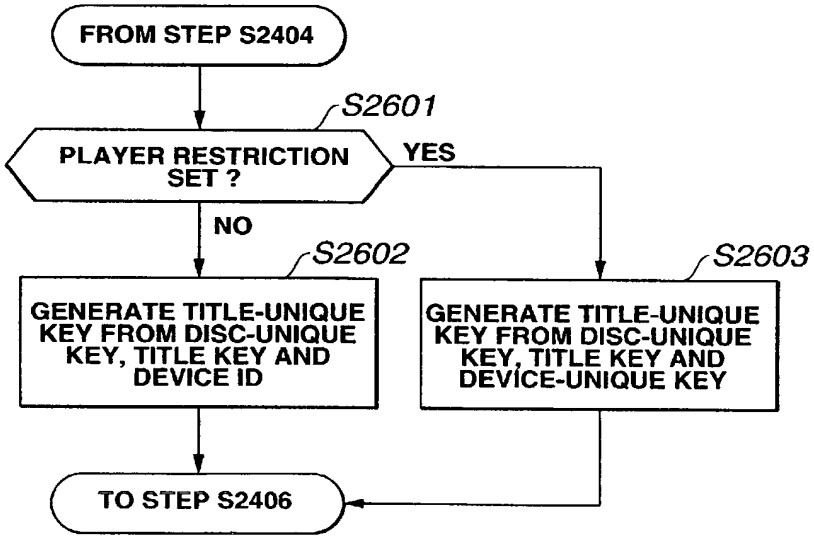

FROM STEP S2404
S2601
PLAYER RESTRICTION SET ?
YES
NO
S2602
GENERATE TITLE-UNIQUE KEY FROM DISC-UNIQUE KEY, TITLE KEY AND DEVICE ID
S2603
GENERATE TITLE-UNIQUE KEY FROM DISC-UNIQUE KEY, TITLE KEY AND DEVICE-UNIQUE KEY
TO STEP S2406

FIG.26

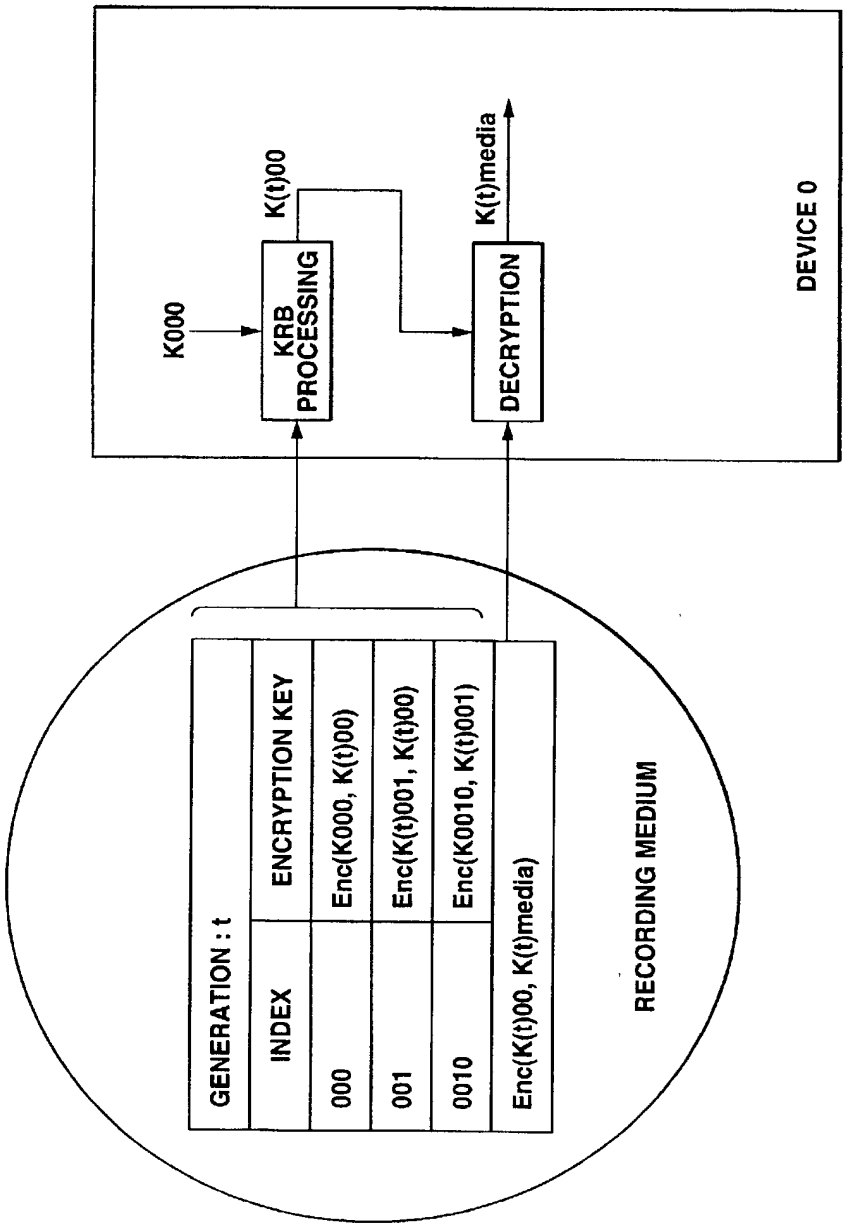

DEVICE 0
K000
KRB PROCESSING
K(t)00
DECRYPTION
K(t)media
RECORDING MEDIUM
GENERATION : t
INDEX
ENCRYPTION KEY
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)media)

FIG.27

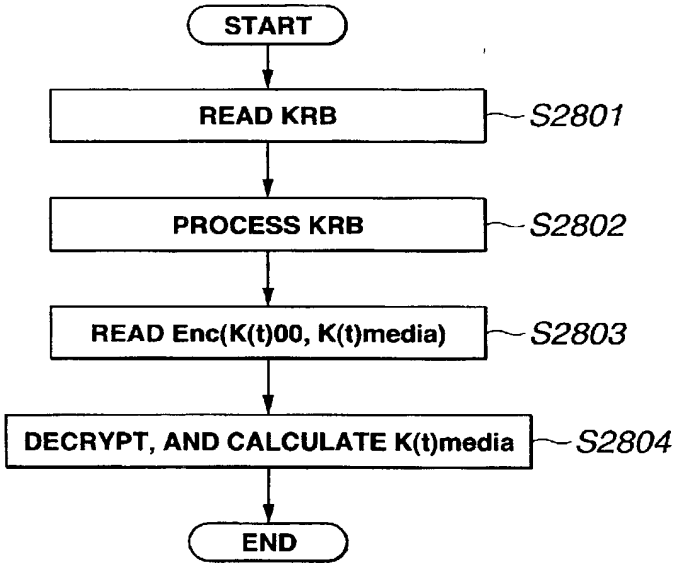

START
READ KRB
S2801
PROCESS KRB
S2802
READ Enc(K(t)00, K(t)media)
S2803
DECRYPT, AND CALCULATE K(t)media
S2804
END

FIG.28

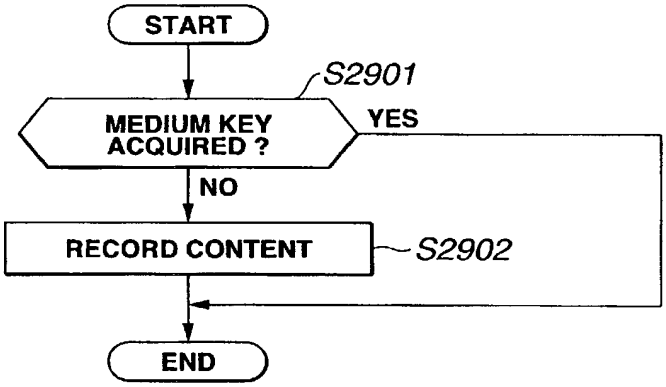

START
S2901
MEDIUM KEY ACQUIRED ?
YES
NO
RECORD CONTENT
S2902
END

FIG.29

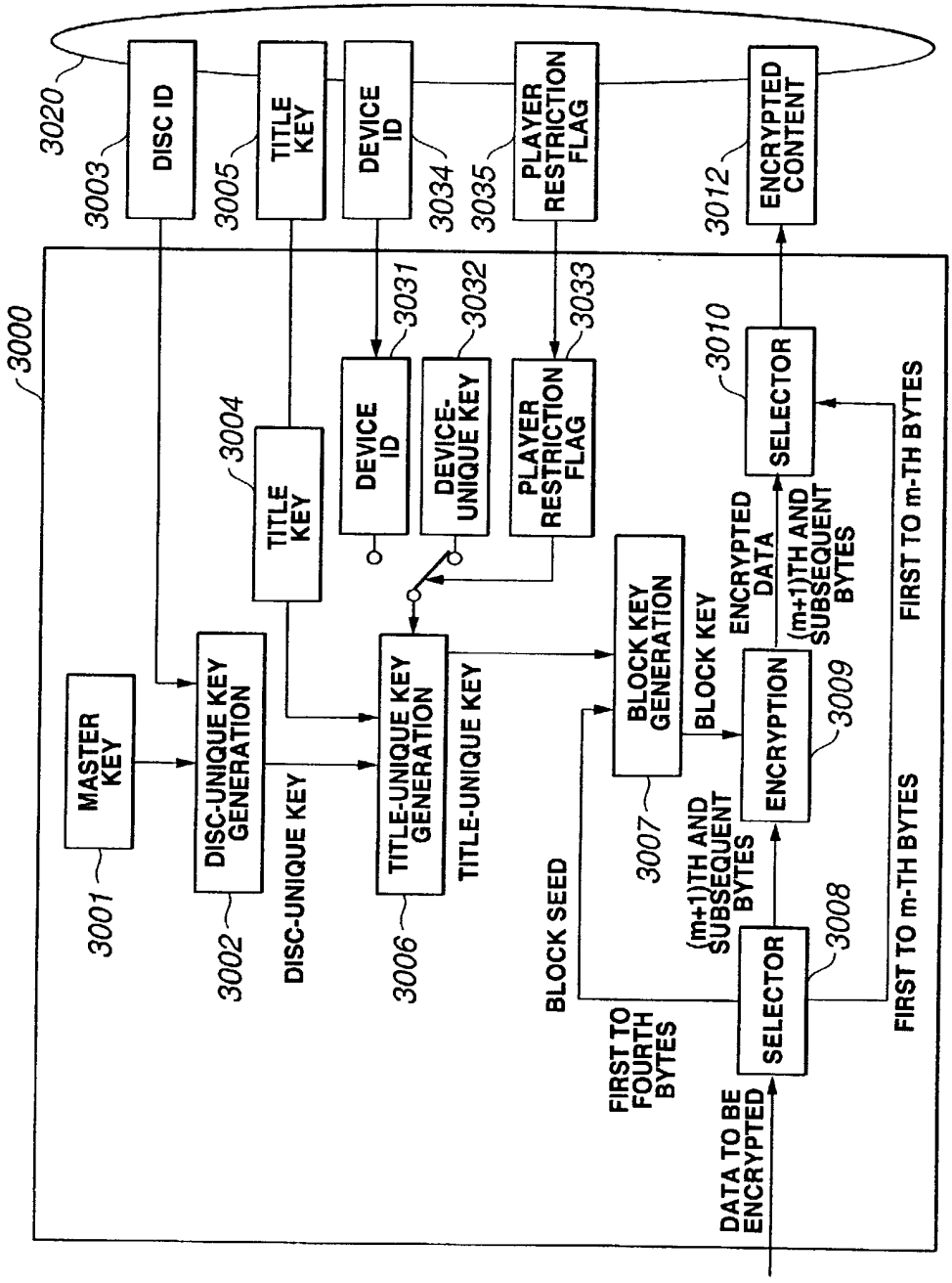

3020
3003
DISC ID
3005
TITLE KEY
3034
DEVICE ID
3035
PLAYER RESTRICTION FLAG
3012
ENCRYPTED CONTENT
3000
3031
3032
3033
3004
TITLE KEY
DEVICE ID
DEVICE-UNIQUE KEY
PLAYER RESTRICTION FLAG
3010
SELECTOR
ENCRYPTED DATA
(m+1)TH AND SUBSEQUENT BYTES
FIRST TO m-TH BYTES
MASTER KEY
3001
DISC-UNIQUE KEY GENERATION
3002
DISC-UNIQUE KEY
TITLE-UNIQUE KEY GENERATION
3006
TITLE-UNIQUE KEY
BLOCK KEY GENERATION
3007
BLOCK KEY
ENCRYPTION
3009
BLOCK SEED
(m+1)TH AND SUBSEQUENT BYTES
FIRST TO FOURTH BYTES
SELECTOR
3008
DATA TO BE ENCRYPTED
FIRST TO m-TH BYTES

FIG.30

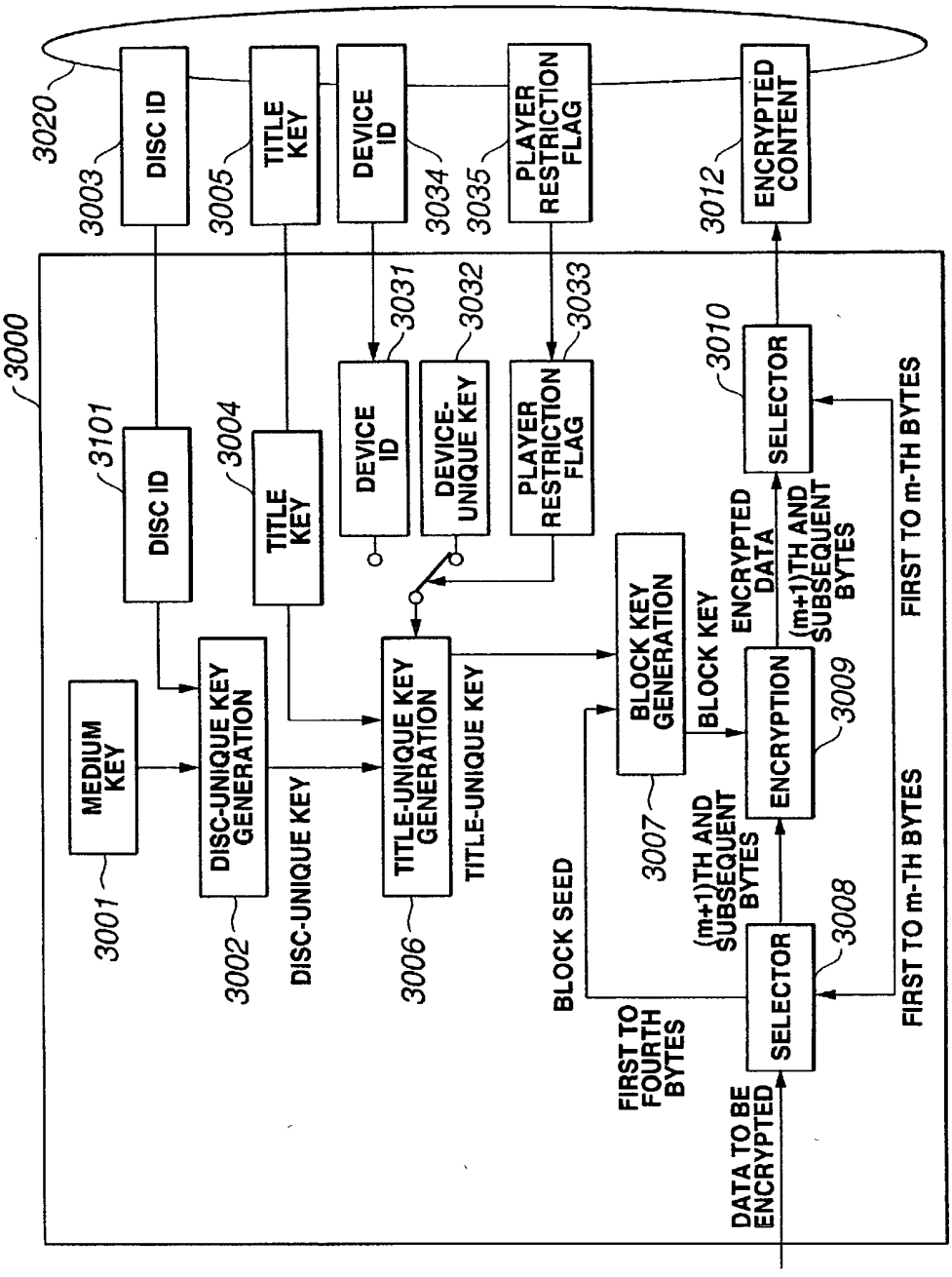

3000
3020
3003
DISC ID
3005
TITLE KEY
3034
DEVICE ID
3035
PLAYER RESTRICTION FLAG
3012
ENCRYPTED CONTENT
3001
MEDIUM KEY
3101
DISC ID
3002
DISC-UNIQUE KEY GENERATION
DISC-UNIQUE KEY
3004
TITLE KEY
3006
TITLE-UNIQUE KEY GENERATION
TITLE-UNIQUE KEY
3031
DEVICE ID
3032
DEVICE-UNIQUE KEY
3033
PLAYER RESTRICTION FLAG
BLOCK SEED
3007
BLOCK KEY GENERATION
BLOCK KEY
(m+1)TH AND SUBSEQUENT BYTES
ENCRYPTION
3009
ENCRYPTED DATA
(m+1)TH AND SUBSEQUENT BYTES
3010
SELECTOR
FIRST TO FOURTH BYTES
SELECTOR
3008
FIRST TO m-TH BYTES
FIRST TO m-TH BYTES
DATA TO BE ENCRYPTED

FIG.31

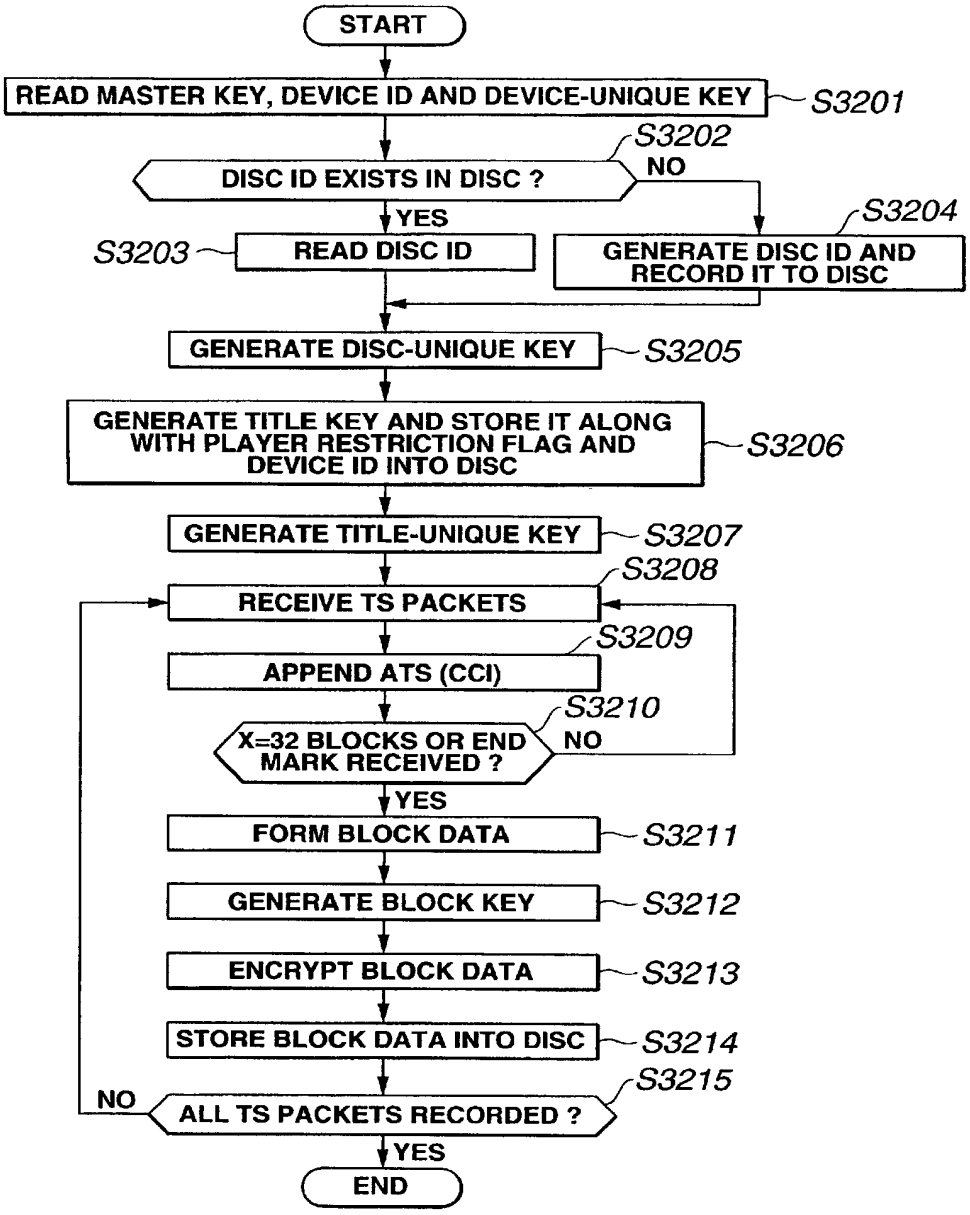

START
READ MASTER KEY, DEVICE ID AND DEVICE-UNIQUE KEY
S3201
S3202
DISC ID EXISTS IN DISC ?
NO
YES
S3203
READ DISC ID
S3204
GENERATE DISC ID AND RECORD IT TO DISC
GENERATE DISC-UNIQUE KEY
S3205
GENERATE TITLE KEY AND STORE IT ALONG WITH PLAYER RESTRICTION FLAG AND DEVICE ID INTO DISC
S3206
GENERATE TITLE-UNIQUE KEY
S3207
S3208
RECEIVE TS PACKETS
S3209
APPEND ATS (CCI)
S3210
X=32 BLOCKS OR END MARK RECEIVED ?
NO
YES
FORM BLOCK DATA
S3211
GENERATE BLOCK KEY
S3212
ENCRYPT BLOCK DATA
S3213
STORE BLOCK DATA INTO DISC
S3214
S3215
NO
ALL TS PACKETS RECORDED ?
YES
END

FIG.32

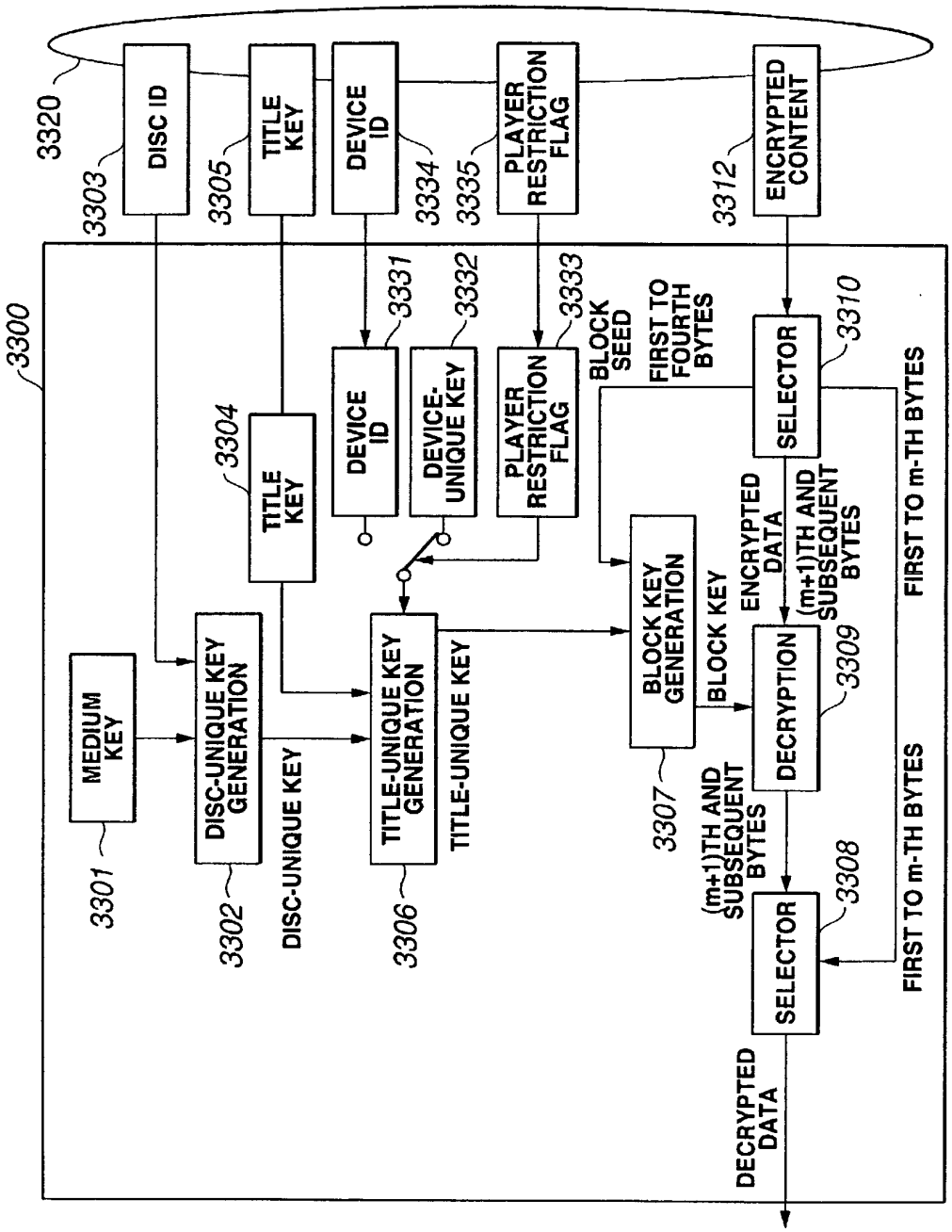

3320
DISC ID
3303
TITLE KEY
3305
DEVICE ID
3334
PLAYER RESTRICTION FLAG
3335
ENCRYPTED CONTENT
3312
3300
3331
3332
3333
BLOCK SEED
FIRST TO FOURTH BYTES
SELECTOR
3310
3304
TITLE KEY
DEVICE ID
DEVICE-UNIQUE KEY
PLAYER RESTRICTION FLAG
MEDIUM KEY
3301
DISC-UNIQUE KEY GENERATION
3302
DISC-UNIQUE KEY
TITLE-UNIQUE KEY GENERATION
3306
TITLE-UNIQUE KEY
BLOCK KEY GENERATION
3307
BLOCK KEY
ENCRYPTED DATA
(m+1)TH AND SUBSEQUENT BYTES
DECRYPTION
3309
(m+1)TH AND SUBSEQUENT BYTES
3308
SELECTOR
FIRST TO m-TH BYTES
FIRST TO m-TH BYTES
DECRYPTED DATA

FIG.33

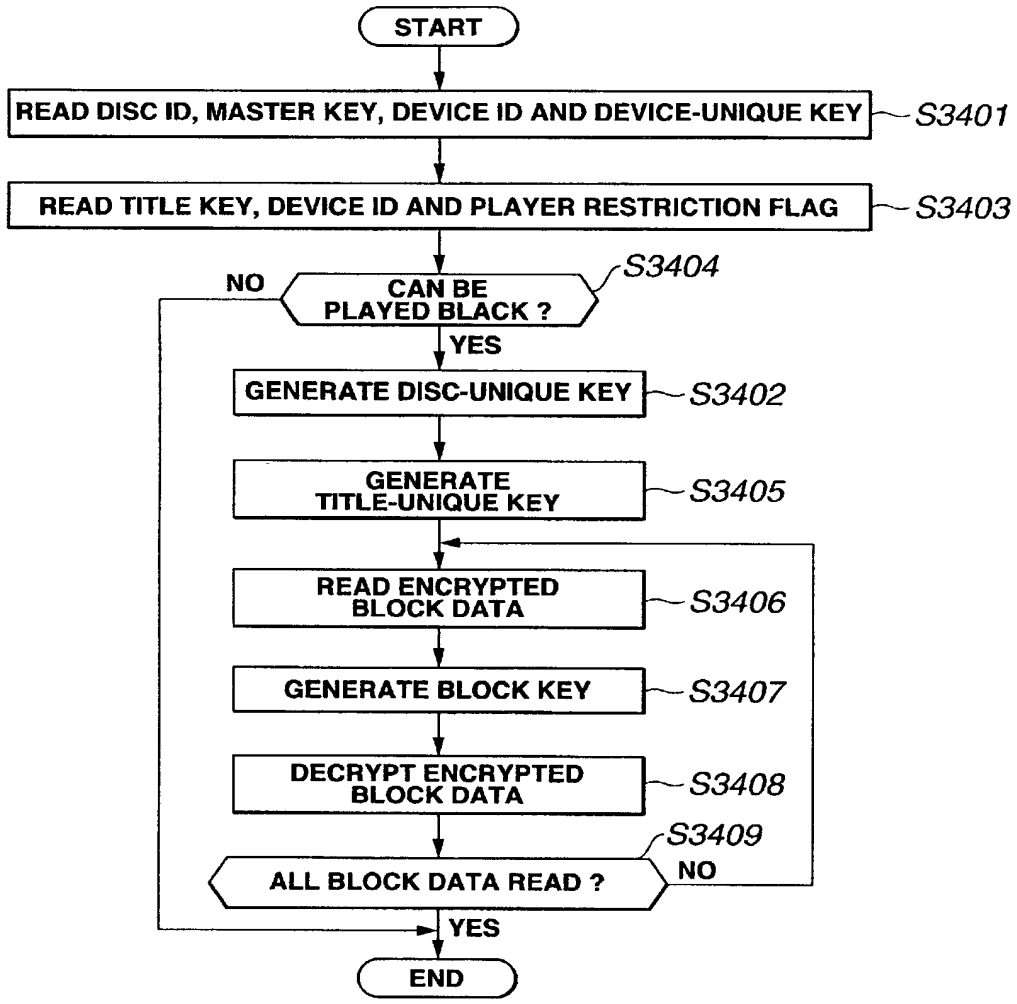

START
READ DISC ID, MASTER KEY, DEVICE ID AND DEVICE-UNIQUE KEY
S3401
READ TITLE KEY, DEVICE ID AND PLAYER RESTRICTION FLAG
S3403
S3404
NO
CAN BE PLAYED BLACK ?
YES
GENERATE DISC-UNIQUE KEY
S3402
GENERATE TITLE-UNIQUE KEY
S3405
READ ENCRYPTED BLOCK DATA
S3406
GENERATE BLOCK KEY
S3407
DECRYPT ENCRYPTED BLOCK DATA
S3408
S3409
ALL BLOCK DATA READ ?
NO
YES
END

FIG.34

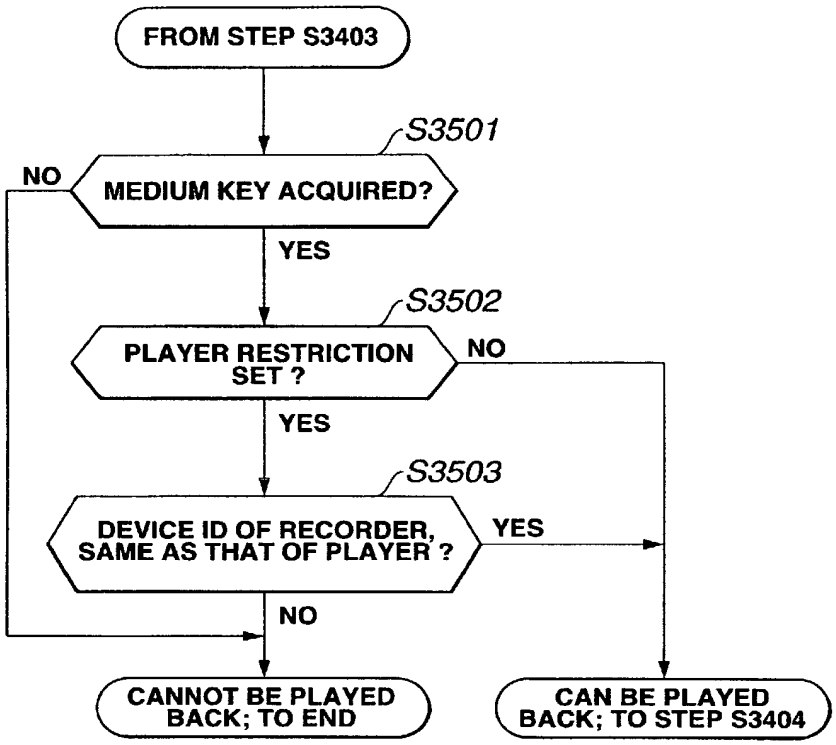

FROM STEP S3403
S3501
NO
MEDIUM KEY ACQUIRED?
YES
S3502
PLAYER RESTRICTION SET ?
NO
YES
S3503
DEVICE ID OF RECORDER, SAME AS THAT OF PLAYER ?
YES
NO
CANNOT BE PLAYED BACK; TO END
CAN BE PLAYED BACK; TO STEP S3404

FIG.35

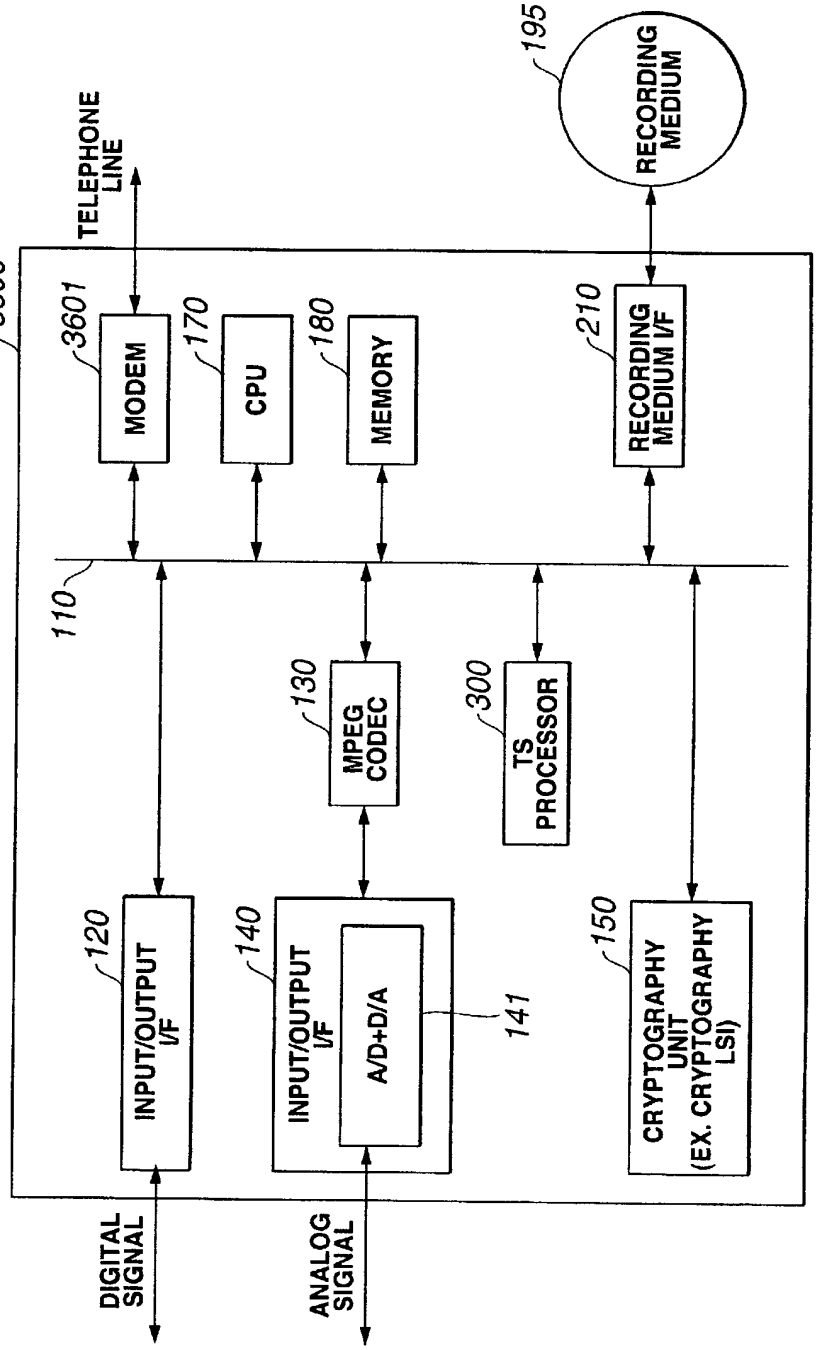

3600
TELEPHONE LINE
195
RECORDING MEDIUM
3601
MODEM
170
CPU
180
MEMORY
210
RECORDING MEDIUM I/F
110
130
MPEG CODEC
300
TS PROCESSOR
120
INPUT/OUTPUT I/F
140
INPUT/OUTPUT I/F
A/D+D/A
141
150
CRYPTOGRAPHY UNIT (EX. CRYPTOGRAPHY LSI)
DIGITAL SIGNAL
ANALOG SIGNAL

FIG.36

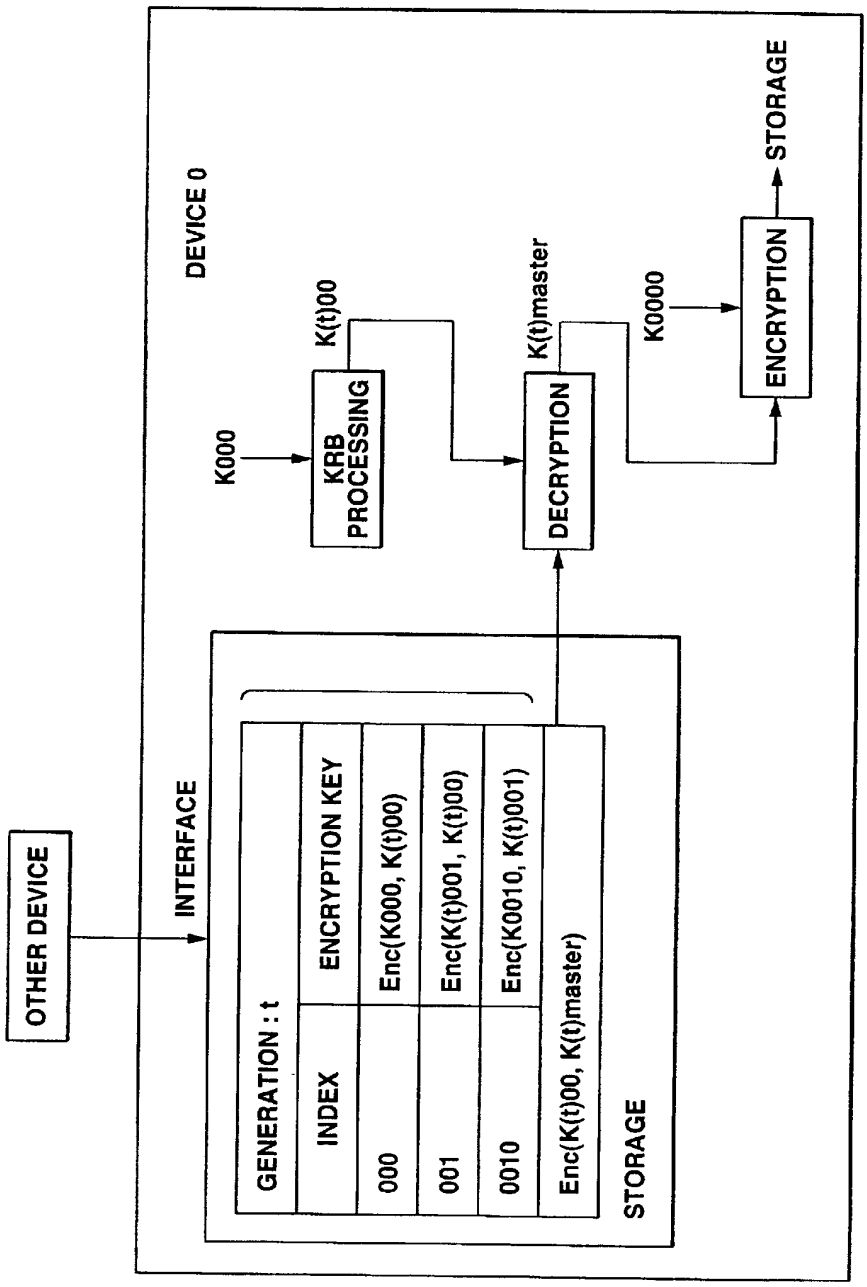

OTHER DEVICE
INTERFACE
DEVICE 0
K000
KRB PROCESSING
K(t)00
K(t)master
DECRYPTION
K0000
ENCRYPTION
STORAGE
GENERATION : t
INDEX
ENCRYPTION KEY
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)master)
STORAGE

FIG.37

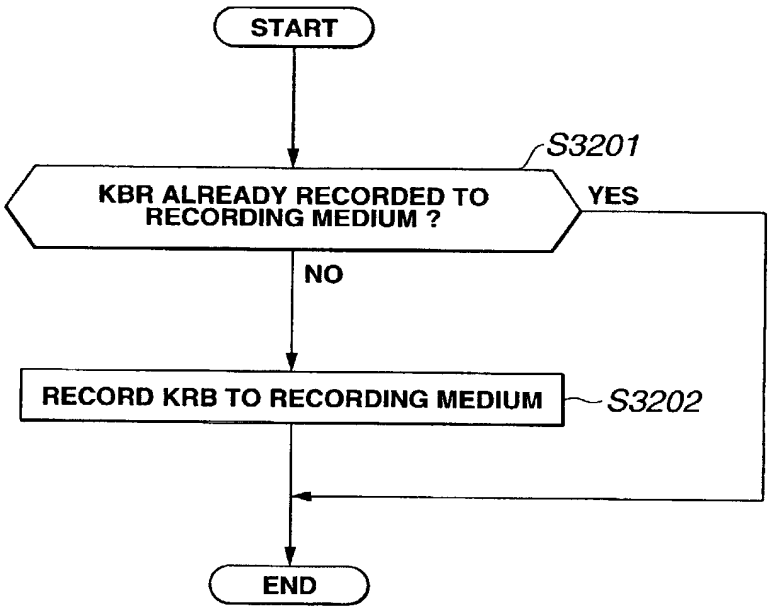

START
S3201
KBR ALREADY RECORDED TO RECORDING MEDIUM ?
YES
NO
RECORD KRB TO RECORDING MEDIUM
S3202
END

FIG.38

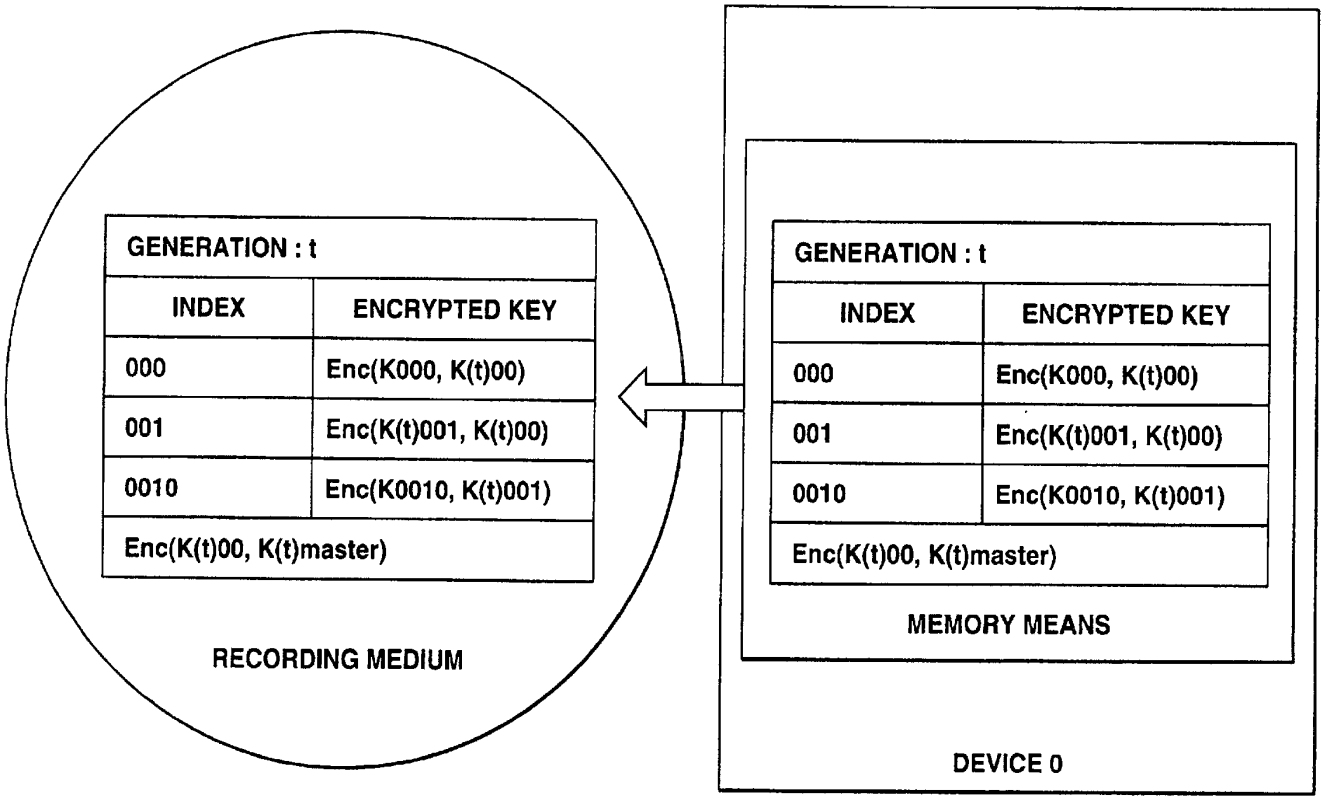


FIG.39

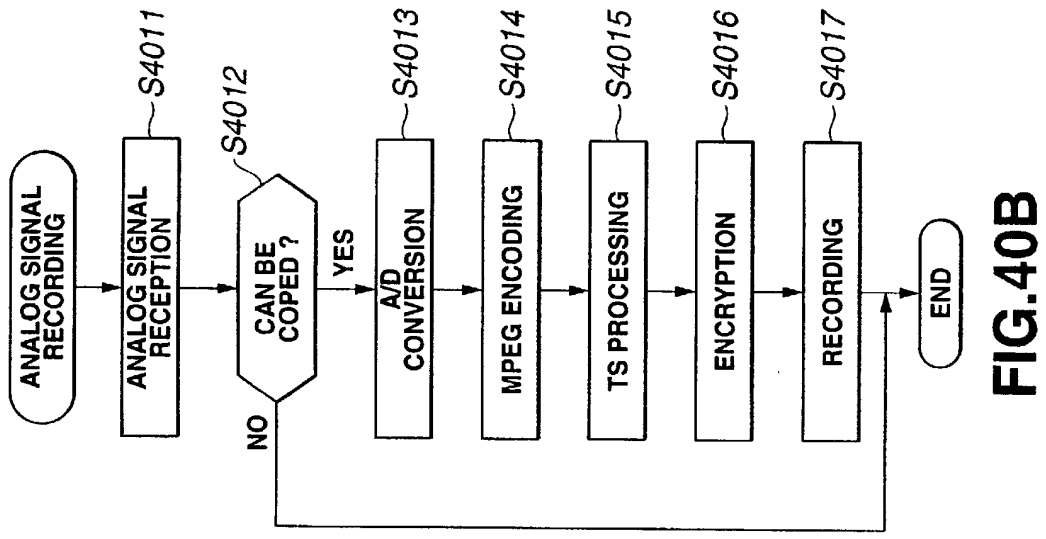


FIG.40B

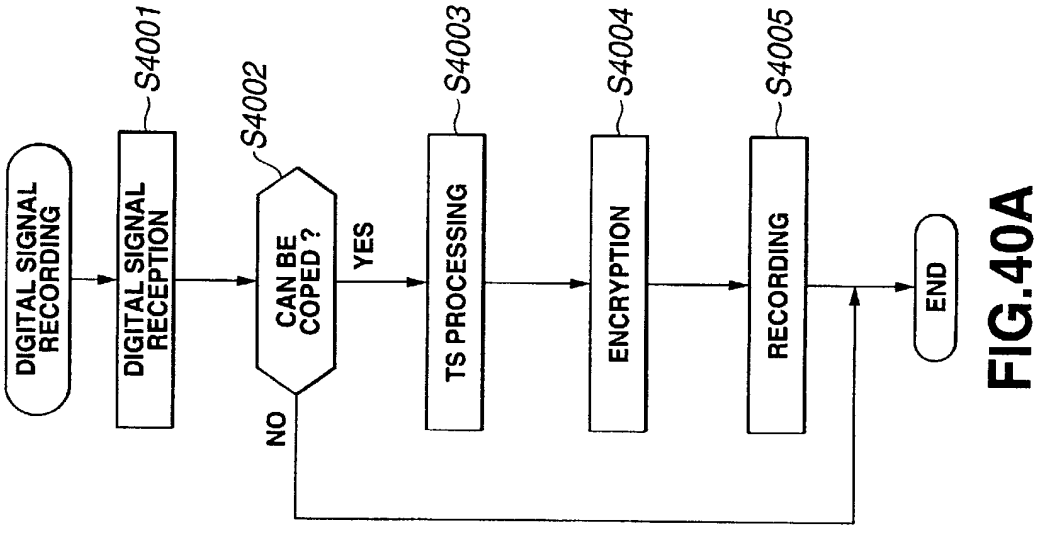


FIG.40A

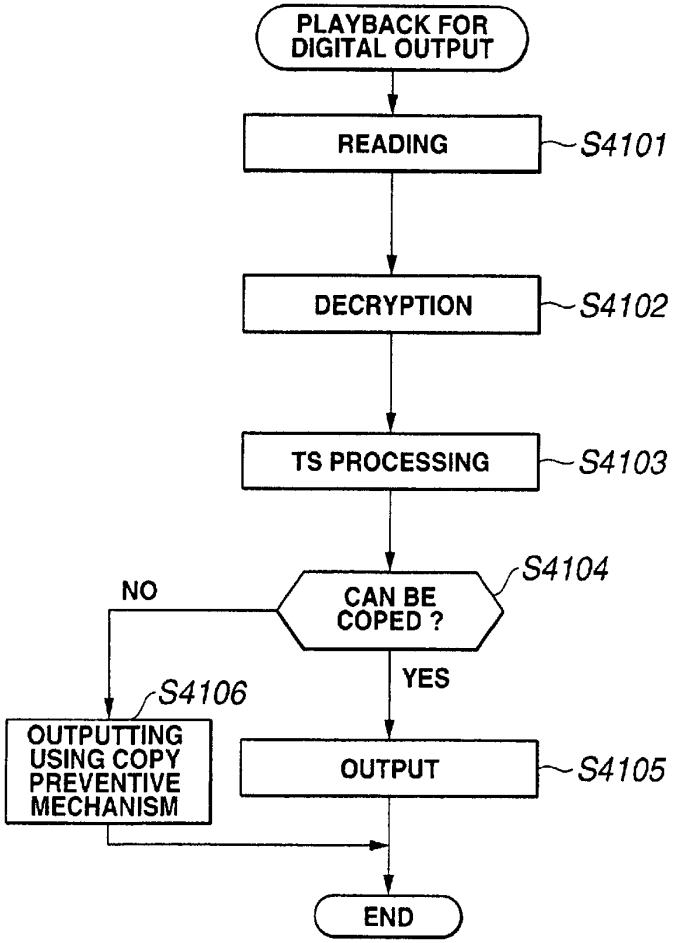


FIG.41A

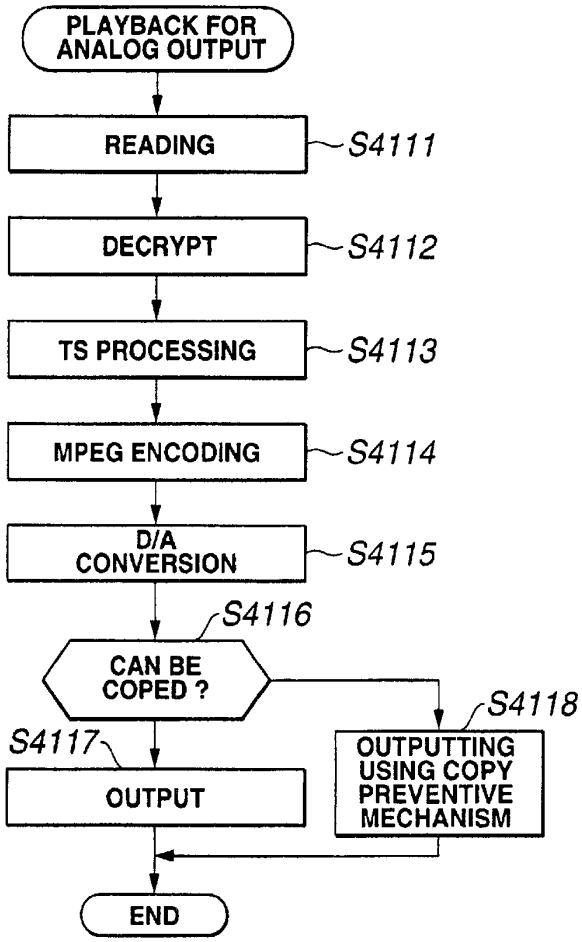


FIG.41B

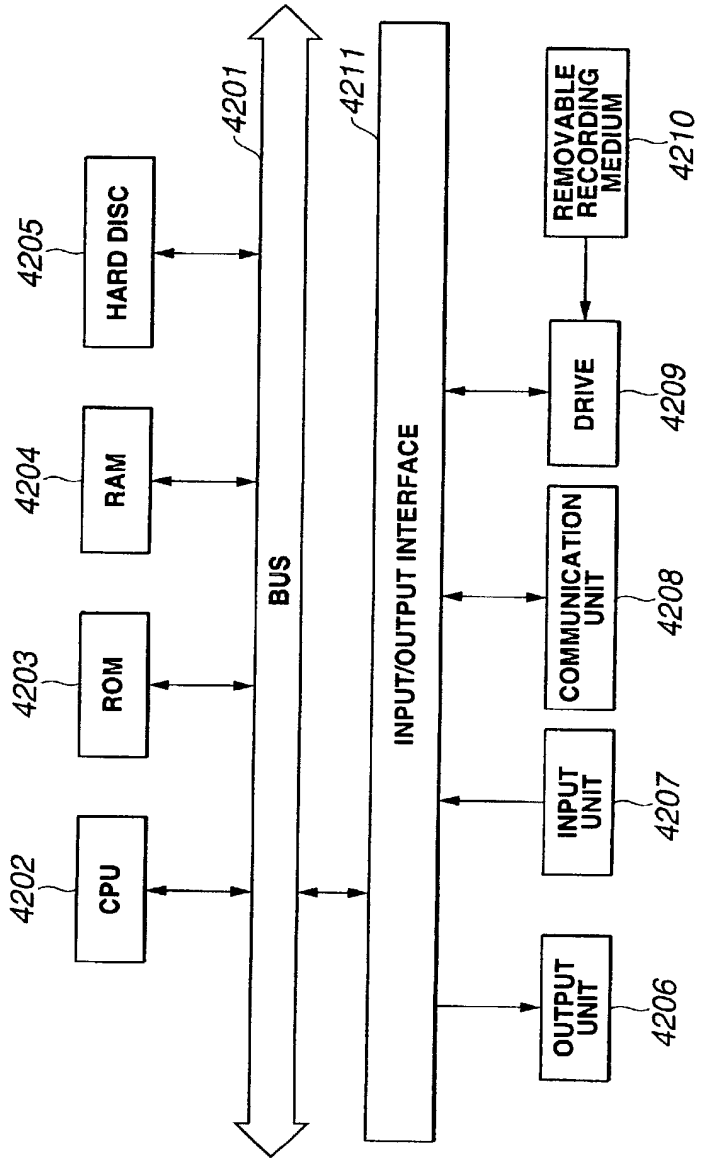

4202
CPU
4203
ROM
4204
RAM
4205
HARD DISC
4201
BUS
4211
INPUT/OUTPUT INTERFACE
4206
OUTPUT UNIT
4207
INPUT UNIT
4208
COMMUNICATION UNIT
4209
DRIVE
4210
REMOVABLE RECORDING MEDIUM

FIG.42

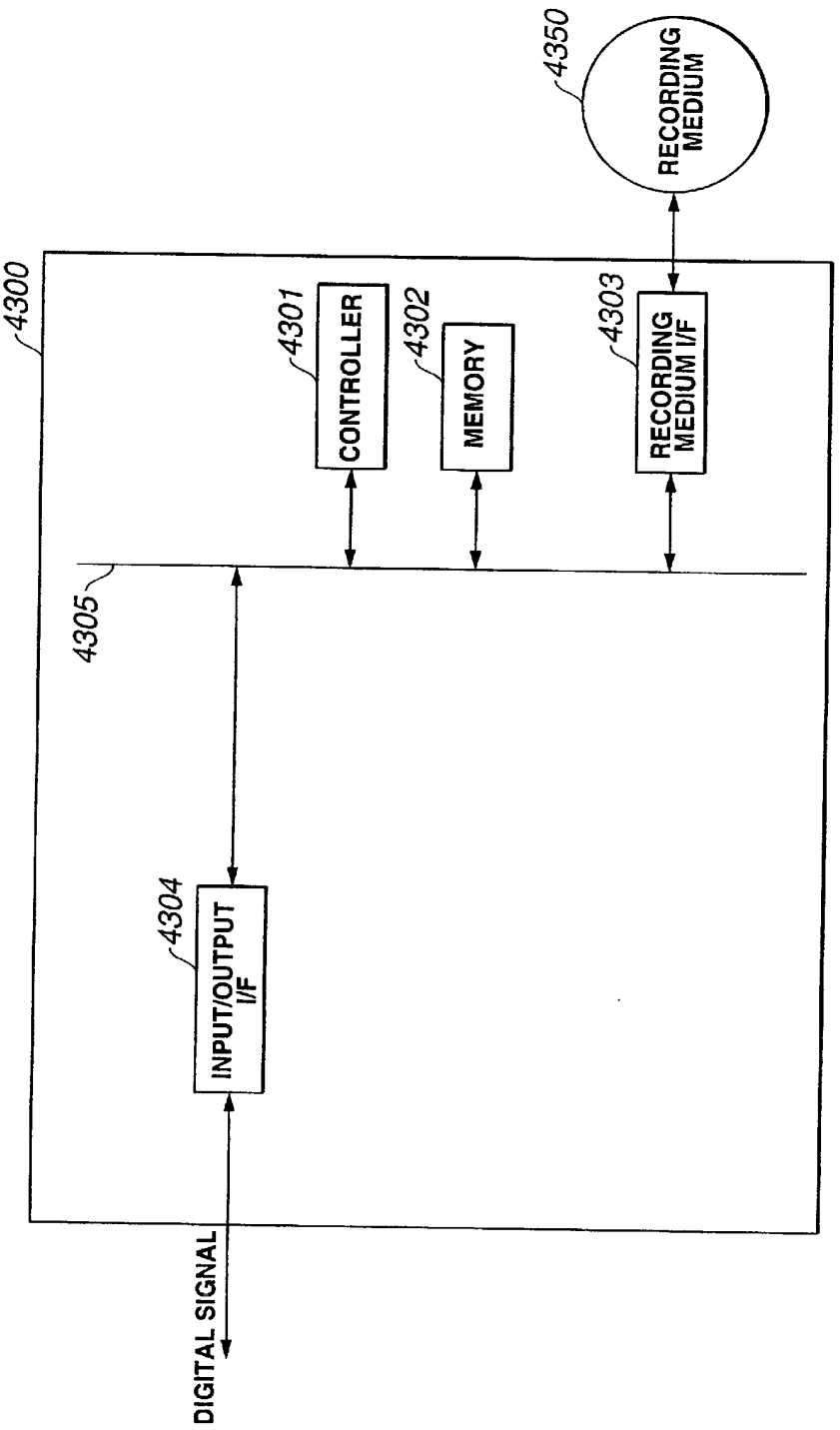

4350
RECORDING MEDIUM
4300
4301
CONTROLLER
4302
MEMORY
4303
RECORDING MEDIUM I/F
4305
4304
INPUT/OUTPUT I/F
DIGITAL SIGNAL

FIG.43

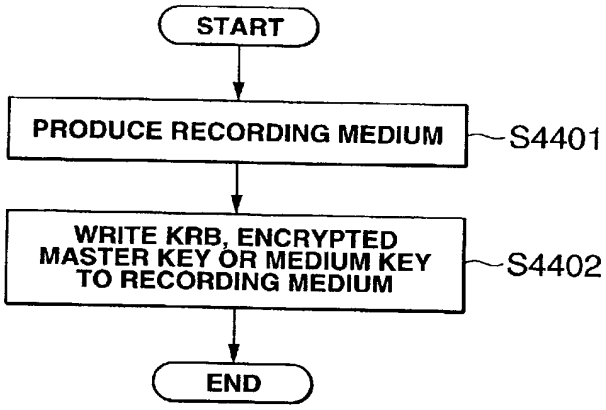

START
PRODUCE RECORDING MEDIUM
S4401
WRITE KRB, ENCRYPTED MASTER KEY OR MEDIUM KEY TO RECORDING MEDIUM
S4402
END

FIG.44

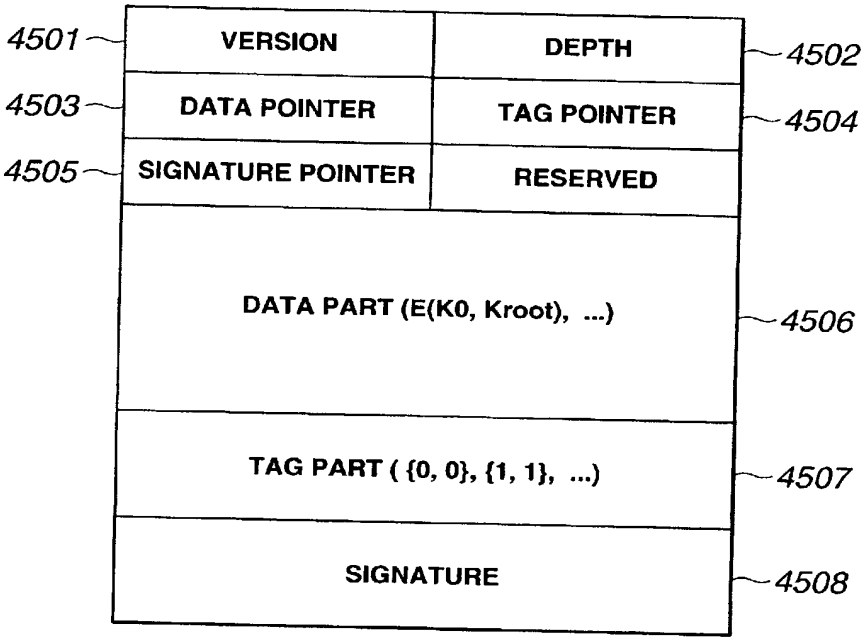

4501
VERSION
DEPTH
4502
4503
DATA POINTER
TAG POINTER
4504
4505
SIGNATURE POINTER
RESERVED
DATA PART (E(K0, Kroot), ...)
4506
TAG PART ({0, 0}, {1, 1}, ...)
4507
SIGNATURE
4508

FIG.45

FIG.46A

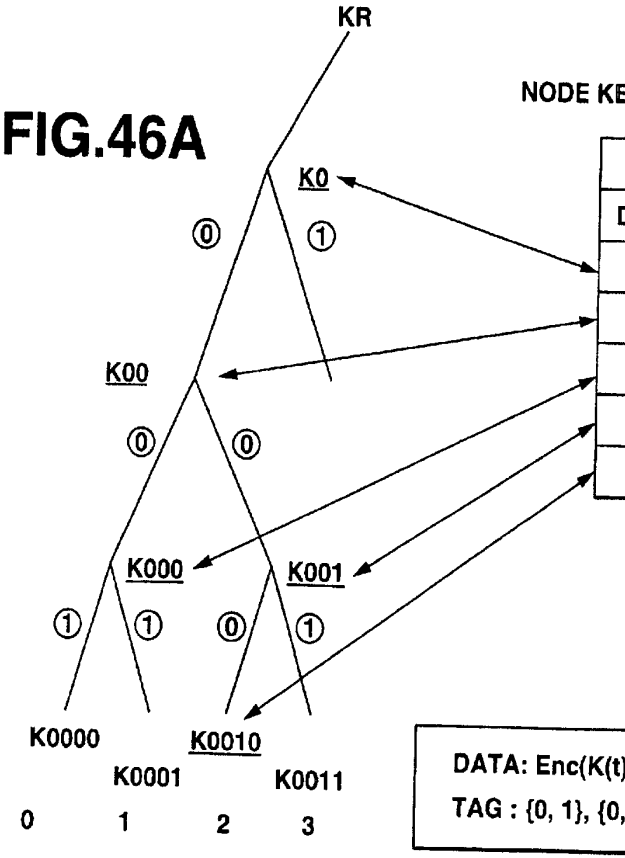


FIG.46B

KRB (KEY RENEWAL BLOCK)

NODE KEY OF VERSION:t IS SENT TO DEVICES 0, 1 AND 2

TOP NODE ADDRESS : KR	
DATA (ENCRYPTION KEY)	TAG
Enc(K(t)0, K(t)R)	{0, 1}
Enc(K(t)00, K(t)0)	{0, 0}
Enc(K000, K(t)00)	{1, 1}
Enc(K(t)001, K(t)00)	{0, 1}
Enc(K0010, K(t)001)	{1, 1}

{LTAG, RTAG}
0 WHEN DATA EXIXTS IN EACH OF DIRECTIONS L AND R;1 WHEN NO DATA EXIXTS

DATA: Enc(K(t)0, K(t)R), Enc(K(t)00, K(t)0), ...
TAG : {0, 1}, {0, 0}, {1, 1}, ...

FIG.46C